INSTALACIÓN, ADMINISTRACIÓN, CONFIGURACIÓN E IMPLEMENTACIÓN DE SERVIDORES LINUX CON ÉNFASIS EN EL DESARROLLO DE UN MODELO ADMINISTRATIVO Y LA CREACIÓN DE UN PROTOTIPO DE CLÚSTER DE ALTA DISPONIBILIDAD.

ALEXANDER BARBOSA AYALA
ELKIN DARÍO MUÑOZ DUARTE

UNIVERSIDAD INDUSTRIAL DE SANTADER
FACULTAD DE INGENIERÍAS FISICOMECÁNICAS
ESCUELA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
BUCARAMANGA
2012

INSTALACIÓN, ADMINISTRACIÓN, CONFIGURACIÓN E IMPLEMENTACIÓN DE SERVIDORES LINUX CON ÉNFASIS EN EL DESARROLLO DE UN MODELO ADMINISTRATIVO Y LA CREACIÓN DE UN PROTOTIPO DE CLÚSTER DE ALTA DISPONIBILIDAD.

ALEXANDER BARBOSA AYALA
ELKIN DARÍO MUÑOZ DUARTE

Trabajo de Grado para optar al título de ingeniero de Sistemas

Director
M.Sc. Manuel Guillermo Flórez Becerra

UNIVERSIDAD INDUSTRIAL DE SANTADER
FACULTAD DE INGENIERÍAS FISICOMECÁNICAS
ESCUELA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
BUCARAMANGA
2012

DEDICATORIA

“No puedes separar la paz de la libertad, porque nadie puede estar en paz, a menos que tenga su libertad”.
Malcolm X

A mis padres Saúl y Magdalena y a mi hermano Javier por su compresión y apoyo incondicional en todo momento de mi vida.

A mi compañero y amigo Elkin Muñoz, que durante todos estos años de carrera ha sido un hermano y ha contribuido en mi crecimiento personal.

A todos mis familiares y amigos, que me han instruido a lo largo de mi vida y con los cuales he compartido momentos gratos y memorables.

Alexander Barbosa Ayala

DEDICATORIA

“La esperanza es cierta espera de la gloria futura, que produce la gracia con el mérito adquirido”

Dante Alighieri – La Divina Comedia, canto XXV

A mis padres William y María y a mi hermano Cristian que me han apoyado en todo momento en cada una de mis decisiones tanto en mi vida profesional como personal.

A mi gran amigo Alexander Barbosa, el cual fue de gran apoyo todo este trayecto de carrera, en especial, tengo el gusto de dedicarle este gran trabajo. Sólo me resta darle las gracias por acompañarme hasta el último día de trabajo.

Por último y no menos importante, a mis amigos y demás familiares que durante la carrera me han guiado y ayudado en todo momento.

Elkin Darío Muñoz Duarte

AGRADICIMIENTOS

Los autores expresan sus agradecimientos:

Al M.Sc. Manuel Guillermo Flórez Becerra, por el apoyo y confianza depositada en nosotros desde el inicio, manteniendo a cada momento una constante disposición al trabajo desarrollado.

A la Universidad Industrial de Santander, por su carácter público y autónomo y a la Escuela de Ingeniería de Sistemas por la formación integral recibida.

A la fundación Raúl Ocazionez por confiar en la investigación y el potencial humano de la Escuela de Ingeniería de Sistemas

A la gran comunidad de software libre, que comparte todos sus proyectos vía web para el uso de tecnologías que crecen con el pasar del tiempo y dan soporte permanente a sus herramientas.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

RESUMEN

TITULO: INSTALACIÓN, ADMINISTRACIÓN, CONFIGURACIÓN E IMPLEMENTACIÓN DE SERVIDORES LINUX CON ÉNFASIS EN EL DESARROLLO DE UN MODELO ADMINISTRATIVO Y LA CREACIÓN DE UN PROTOTIPO DE CLUSTER DE ALTA DISPONIBILIDAD.*****

AUTORES: BARBOSA AYALA, Alexander. MUÑOZ DUARTE, Elkin Darío******

PALABRAS CLAVE: Administración, alta disponibilidad, clúster, modelo, seguridad.

DESCRIPCIÓN:

Al contarse con nuevos equipos servidores para la prestación de servicios en la Escuela de Ingeniería de Sistemas e Informática de la Universidad Industrial de Santander, se hizo necesario instalar y configurar todo el software necesario para que estos operen adecuadamente, según las condiciones del entorno de producción. De igual manera, los servicios ofrecidos hacia los usuarios, deben contar con una infraestructura de seguridad y disponibilidad adecuada, para que su uso sea confiable.

En este proyecto se describe cada software instalado en los equipos, así como los aspectos tenidos en cuenta para la configuración de seguridad y operatividad de los mismos. Además, se muestra el proceso de implementación de una infraestructura de clúster de alta disponibilidad y los procesos de pruebas al cual fue sometido en un entorno real y simulado. Es importante resaltar que todo el software utilizado en los procesos anteriormente mencionados es de carácter libre, a pesar de la existencia de software privativo que tiene la misma funcionalidad.

Además, se hizo necesario organizar todos los procedimientos que abarcan la gestión de los equipos, mediante la implementación de una base normativa y un modelo de administración, abordando el proceso administrativo desde una perspectiva organizacional, teniendo en cuenta los aspectos funcionales del entorno de trabajo.

En general, con el presente trabajo los usuarios podrán contar con servicios orientados a la web, soportados en dos servidores trabajando de manera conjunta, mediante una estructura de alta disponibilidad y bajo una normativa administrativa.

---

* Trabajo de Grado

** Universidad Industrial de Santander, Facultad de Ingenierías Físico-Mecánicas, Escuela de Ingeniería de Sistemas. Director, MANUEL GUILLERMO FLÓREZ BECERRA

ABSTRACT

TITLE: INSTALLATION, ADMINISTRATION, CONFIGURATIONS AND IMPLEMENTATION OF LINUX'S SERVERS WITH ÉNPHASIS IN DEVELOPMENT OF AN ADMINISTRATIVE MODEL AND THE CREATION OF A HIGH AVAILABILITY CLUSTER'S PROTOTYPE.*

AUTHORS: BARBOSA AYALA, Alexander. MUÑOZ DUARTE, Elkin Darío**

KEY WORDS: Administration, high availability, cluster, model, safety.

DESCRIPTION:

Counting with new server's equipment to provide the services at the School of Systems Engineering and Informatics, Industrial University of Santander, it was necessary to install and configure all the software needed so they can work properly, according to production environment conditions. Equally, the services offered to users, have to count with an appropriate safety and availability infrastructure.

In this project is described every software installed on the servers, as well the aspects we based on the safety and operability configurations for them. Besides, is shown the implementation process of a high availability Cluster's infrastructure and the testing processes which it was subjected in a real and simulated environment. It is important to note that all the software used in the process mentioned before is of free feature, despite of existence of privative software with the same functionality.

Besides, it was necessary organize all procedures covering the management of equipment, by the implementation of a normative base and an administration model, taking the administrative process from an organizational perspective, considering the functional aspects working environment.

In general, with this work the users can count with web-oriented services, supported in two servers working together, through a high availability structure and under administrative norms.

---

* Thesis

** Universidad Industrial de Santander, Facultad de Ingenierías Físico-Mecánicas, Escuela de Ingeniería de Sistemas. Director, MANUEL GUILLERMO FLÓREZ BECERRA

INTRODUCCIÓN

Con la llegada de nuevos equipos de servidores para el soporte de los servicios web ofrecidos por la EISI (Escuela de Ingeniería de Sistemas e Informática), es indispensable contar con una planeación adecuada para el uso correcto de dicho hardware, con lo cual se puede garantizar la disponibilidad de los recursos y la seguridad de los equipos.

Lo anterior se contempla desde un modelo de administración en el cual se incluyan diferentes parámetros y demás características que brinden la posibilidad de mantener la administración y la disponibilidad de los diferentes recursos, tanto hardware como software, para los usuarios y teniendo en cuenta la posibilidad de entrada de nuevos servicios web según sea la demanda de usuarios y necesidades que se den a futuro en la EISI; es decir, los equipos deben tener soporte de los servicios actuales y estar en la capacidad de albergar nuevos, brindando la posibilidad a futuros investigadores a que disponga también de éstos recursos.

Por tanto, el presente proyecto se enfoca en primera instancia en la migración de los servicios web desde los antiguos servidores a los nuevos, buscando la forma de hacer este proceso lo más transparente posible para los usuarios, seguido de un proceso de investigación y puesta a punto del modelo de administración ya mencionado. Finalmente, se buscará investigar e implementar un diseño de clúster de alta disponibilidad con el cual se logra garantizar que los recursos estén accesibles para los usuarios.

Con los parámetros mencionados se busca en general garantizar la optimización de la labor administrativa en los nuevos equipos de servidores, haciendo posible que se hagan relevos de administradores de manera oportuna y correcta, teniendo en cuenta que la labor administrativa se lleva a cabo por estudiantes de pregrado de último nivel de Ingeniería de Sistemas.

1. DESCRIPCIÓN GENERAL

1.1 OBJETIVOS

1.1.1 Objetivos Generales

- Migración, administración, mantenimiento y seguridad aplicados a servidores Linux en la Escuela de Ingeniería de Sistemas.
- Diseñar un prototipo para implementación de un clúster de alta disponibilidad, apoyados en herramientas actuales de software libre.

1.1.2 Objetivos Específicos

- Administración, mantenimiento, monitoreo y recuperación del servidor de producción en caso de fallas.
- Configurar y Migrar los actuales servicios en producción.
- Implementar políticas y mecanismos de seguridad para garantizar la confiabilidad e integridad de los recursos disponibles.
- Organizar las diferentes tareas administrativas:
    - Generación automática de backups de los sitios web y de la base de datos acorde con una política de seguridad.
    - Automatización de los procesos relacionados con la administración del servidor.
    - Actualizaciones del kernel del S.O.
    - Análisis y seguimiento de los registros o logs del sistema.
    - Definición y creación de perfiles de usuarios.
    - Creación de usuarios enjaulados.
- Realizar manuales de funciones y procedimientos de:
    - Administración del servidor.
    - Mantenimiento preventivo.
    - Mantenimiento correctivo.

Incluyendo aspectos como políticas de seguridad, perfiles de usuarios, tareas de monitoreo, normas de administración y relevos administrativos.

- Diseñar un prototipo de clúster de alta disponibilidad para garantizar disponibilidad de los recursos y servicios en casos de fallas. Efectuar procesos de verificación de funcionalidad del clúster de alta disponibilidad estudiando su comportamiento en el entorno.
- Entrenamiento de los relevos-administradores que den continuidad a la administración de los servidores.

1.2 JUSTIFICACIÓN

Los procesos de administración en los nuevos servidores sistemas y delfin, deben contar con una adecuada planeación, desde la cual se tenga en cuenta los diferentes aspectos operacionales junto a su respectivo análisis e investigación, para que de esta manera, la puesta en funcionamiento de estos equipos en el entorno producción, ofrezca de forma efectiva y transparente los servicios a la comunidad de la Escuela de Ingeniería de Sistemas e Informática.

Para la correcta definición del perfil administrativo, es importante la creación de un manual de funciones y procedimientos, donde se clarifique diversas funciones administrativas, dando así mayor seguridad al sistema que se encuentra en producción, y por tanto, se asegura una continuidad en la administración, ya que el equipo humano irá cambiando.

Además, para mantener los servicios planeados con proyección hacia futuro, es necesario contar con una infraestructura de hardware óptima, es por esto, que la adquisición de estos nuevos equipos va acorde a dicho fin, ya que los servicios son implantados en equipos con mejores características, a partir de un proceso de migración controlado y cuidadoso.

Los procesos básicos que se hacen de manera mecánica en la labor administrativa, son automatizados con el fin de ayudar a invertir menor cantidad de tiempo en la realización de dichas tareas, con lo cual, es de vital importancia, asegurar la confiabilidad de este proceso a la hora de implementarse, permitiendo

al administrador invertir más tiempo en labores de investigación y monitoreo del sistema.

Un sistema de backup es importante a la hora de tener respaldos de la información vital en una organización, no sólo de las bases de datos sino de los recursos en general, por esto implementar políticas de copias de seguridad es importante ya que en caso de situaciones imprevistas se pueden contar con puntos de control para volver a un estado anterior.

La seguridad es inherente a cualquier sistema susceptible a fallos o ataques, con lo cual es importante mantener en constante monitoreo los diferentes recursos del sistema, así la implementación de un esquema de seguridad, reducirá las probabilidades que sea vulnerado, al mínimo.

Contar con un sistema de alta disponibilidad es una característica muy importante a la hora de prestar un servicio, ya que, el sistema debe estar en capacidad de asegurar la disponibilidad de sus recursos hacia los clientes en cualquier momento, y así su acceso se daría de manera transparente y no se detendría por fallas a nivel de infraestructura.

1.3 VIABILIDAD

Dada la disponibilidad de los nuevos recursos adquiridos para la renovación del campo de servidores en la Escuela de Ingeniería de Sistemas y dado a la creciente demanda de usuarios de dichos recursos, esto se puede satisfacer con la puesta en marcha de un clúster de servidores configurados con una arquitectura basada en la alta disponibilidad, desarrollado e implementado con el uso de herramientas de software libre, que cuentan con soporte web, dispuesto por una gran comunidad que apoya y desarrolla el uso de este tipo de aplicaciones.

Además, con el uso de software libre bajo licencia GNU, los costos se trasladan directamente a la parte investigativa y al proceso de desarrollo del clúster como tal, ya que tanto la instalación como el proceso de aprendizaje, conlleva tiempo y

disposición tanto del director como de los desarrolladores del proyecto y dado a que el hardware se encuentra a disposición, los gastos serían de mantenimiento futuro, si se consideran los costos a nivel de máquina.

Para el usuario, es transparente el uso de los servicios que proveen los servidores de la Escuela de Ingeniería de Sistemas, ya que con la implementación de una administración regulada y controlada, y a su vez de una alta disponibilidad se asegura que los servicios se entreguen de manera permanente a pesar de que se puedan presentar fallas en cualquiera de los equipos que integren el clúster.

2. INSTALACIÓN Y CONFIGURACIÓN DE LOS SERVIDORES

2.1 ESPECIFICACIONES TÉCNICAS

Para la realización del presente proyecto, se ha contado con dos servidores marca Dell, con capacidad de memoria considerable y de Entrada/Salida, desempeño óptimo para gestión de virtualización y bases de datos, además de otras especificaciones técnicas que son de dominio privado. Cada servidor contará con un nombre, con el cual se puede diferenciar cuando se encuentren en producción conectados a internet. El servidor principal cuenta con el nombre *"sistemas"*, asociado al dominio *"sistemas.uis.edu.co"*, y el servidor de apoyo se le asignó el nombre *"delfín"*, asociado al dominio *"delfin.uis.edu.co"*.

2.2 SISTEMA OPERATIVO (DEBIAN 6 SQUEEZE)

Los servidores, al ser equipos nuevos, inicialmente no contaban con ninguna configuración software ni de sistema operativo, por tanto, la labor administrativa se inició desde la instalación misma del S.O. El sistema operativo elegido para el funcionamiento de los servidores fue Debian 6 de 64 bits, que es un S.O basado en GNU/Linux y la fecha de lanzamiento de esta versión fue el 6 de febrero de 2011.

Se optó por la instalación de Debian 6, no sólo por contar con gran popularidad al ser una de las distribuciones de Linux más utilizadas como Sistema Operativo de servidores web en el mundo, sino por ser un S.O estable, por su versatilidad en el mantenimiento e instalación de paquetes software, tiene un bajo consumo de recursos (Memoria Ram, Disco duro, Procesador) de su sistema base, además de tener gran soporte y documentación, entre otros factores que ayudaron decidir su instalación.

Debian 6 como característica relevante, cuenta con un núcleo de Linux completamente libre. Sin embargo, todo el firmware privativo se incluye en los

paquetes *"non-free*" de los repositorios, éstos no se encuentran activados de manera predeterminada, pero se pueden instalar posteriormente. Además, cuenta con la versatilidad de ser multiplataforma, ya que en su versión estable soporta 12 plataformas de arquitectura, entre las más importantes se encuentran la i386 (x86-32), amd64 (x86-64), entre otras.

Los paquetes de software de Debian son organizados por ramas. Los paquetes en desarrollo son puestos en la web oficial en unas ramas llamadas inestable (unstable) y experimentales. Normalmente, los paquetes de software pasan de experimental a inestable de acuerdo a las versiones lanzadas estables por el desarrollador original de la aplicación, pero con el empaquetado y otras modificaciones específicas de Debian introducidas por los desarrolladores. El software que es inestable, pero que no se encuentra listo para estar en la rama inestable, se pone típicamente en la sección experimental. Los paquetes en su versión estable (stable), cuentan con el apoyo del Equipo de Seguridad de Debian y son los recomendados para uso en producción. También dispone de paquetes antiguos o de versiones anteriores en la rama old-stable que se pueden descargar de sitio de repositorios de la página oficial de debían (http://www.debian.org/).

El proyecto Debian fue fundado en el año 1993 por Ian Murdock. Él fue el autor del manifiesto de Debian, el cual muestra la filosofía de desarrollo de la distribución Linux Debian. Dentro de este texto, se destacan aspectos fundamentales, tales como, mantener la distribución abierta coherente a la filosofía del núcleo Linux y de GNU. Actualmente la versión estable es la Debian 6 (squeeze), la anterior, lanzada 14 de febrero de 2009, es la Debian 5 (lenny), y la versión en desarrollo es la Debian 7 (wheezy), aún sin fecha de lanzamiento fijada. Los nombres de las versiones de Debian GNU/Linux son tomados de la película Toy Story.

Cuenta además con licencia GPL (General Public Licence), es de libre distribución y es desarrollado por más de mil voluntarios alrededor del mundo, que colaboran a

través de Internet, colocando su documentación, mejoras, características y cambios realizados en las diferentes versiones en el sitio web oficial de debían.

2.3 SERVIDORES WEB

2.3.1 Servidor Web Apache 2

Dentro de los requerimientos que se han dispuesto para la configuración de los equipos, se especificó contar con dos servidores apache en cada uno, para soportar sitios web con diferentes especificaciones de funcionamiento; para ello, se decidió instalar, tanto en el servidor Sistemas con el servidor Delfín, la versión empaquetada, es decir, el paquete software que se encuentra dentro de los repositorios oficiales de Debian, llamado Apache2 y de igual manera se instaló la versión del Apache HTTP2.2 Web Server para compilación en sistemas Linux.

Apache es un servidor web HTTP de código abierto, instalable en plataformas UNIX (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh entre otras. Éste servidor, se encuentra diseñado de manera modular, es decir, con un núcleo y diversos módulos que le aportan la funcionalidad necesaria para el funcionamiento del servicio. Cuando está operando, se ejecuta como un servicio (demonio) independiente, creando un conjunto de procesos o hilos para manejar las peticiones del servicio.

Como servidor web, es uno de los más populares en su uso en los diferentes dominios que se encuentran en internet, dado a sus características como estabilidad, robustez, administración, tiene buen soporte y documentación, por ser un software libre, entre otros, que lo hacen el servidor web más utilizado y más ampliamente conocido en el mundo, como se puede apreciar en las siguientes gráficas, en las cuales se puede visualizar estadísticas desde enero de 1996 hasta octubre de 2011.

La figura 1, muestra la cuota de mercado de los Servidores web más utilizados en porcentajes y la segunda gráfica muestra el uso de los servidores web en relación a la cantidad de sitios de web activos en internet.

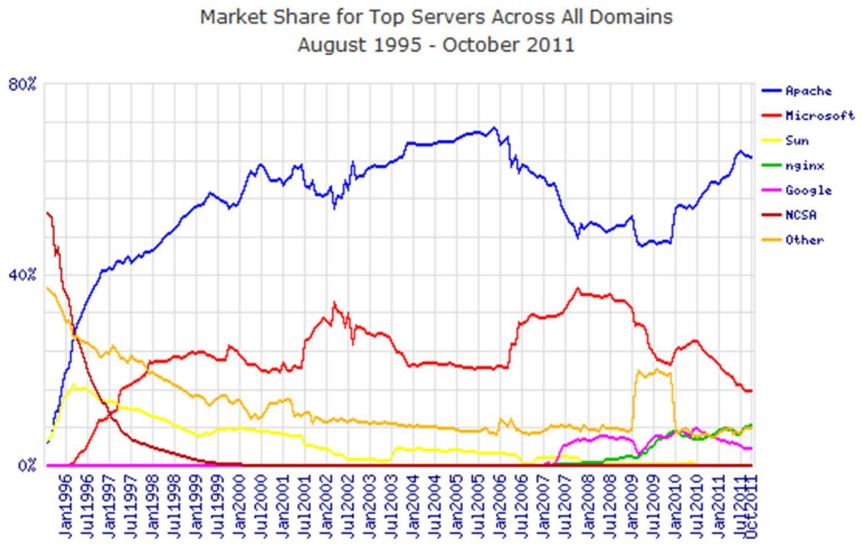

Figura 1 Estadística del uso de servidores. Fuente: http://news.netcraft.com

El Servidor Apache cuenta con gran aceptación en la web como servidor Http, siendo éste el más utilizado en los sitios web mundiales, ya que se encuentra instalado como servidor web en más 60% de los dominios de internet, manteniendo su liderazgo desde junio de 1996 aproximadamente y teniendo su punto de uso más alto en julio de 2005.

En cuanto a la cantidad de sitios web visibles en internet en relación al servidor web que implementan, apache lidera con aproximadamente cien millones de sitios web hacia octubre de 2011 y le sigue en segundo lugar Microsoft con veinte millones de sitios web aproximadamente, como se visualiza en la Figura 2.

Las estadísticas muestran que el servidor Apache es la alternativa más implementada y más aceptada a nivel mundial. Tiene a su favor que es una alternativa libre, estable y robusta. Es desarrollado, actualizado y documentado en comunidad por colaboradores alrededor de todo el mundo.

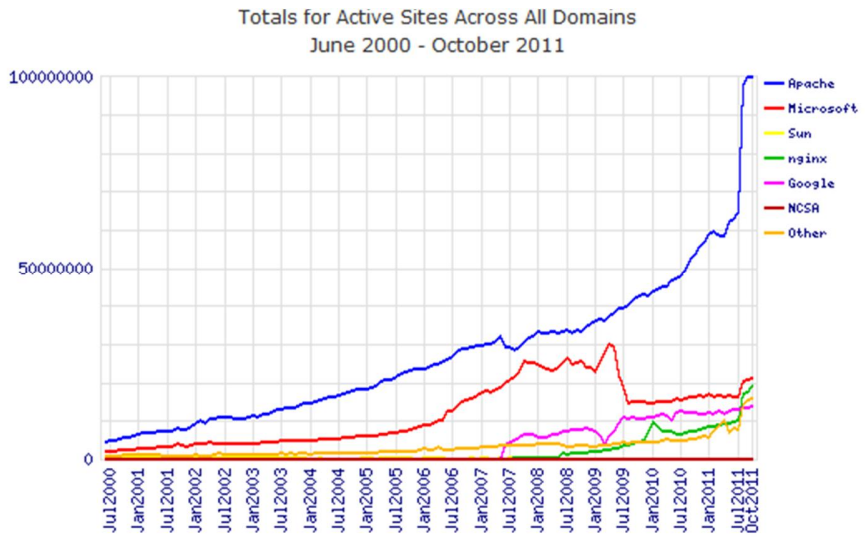

Figura 2 Estadística Cantidad de dominios por Servidor web. Fuente: http://news.netcraft.com

2.3.2 Servidor Web Apache Tomcat 6

La instalación del servidor Tomcat 6 se ha realizado con el fin de dar servicios de ejecución a los sitios web alojados en los equipos, cuyo contenido cuenta con aplicaciones en Java (servlet) y Java Server Pages (JSP).

Los Java servlet son objetos que corren en las páginas web, que son ejecutados como los applet creados en código Java. El propósito de estos servlets, es generar páginas web de forma dinámica y según sean los parámetros de petición que se hagan desde el navegador web se realiza la ejecución del código java. De igual forma, las Java Server Pages (JSP), es una tecnología Java con la cual es posible generar contenido dinámico web por medio de documentos HTML, XML o de otro tipo.

El desarrollo y mantenimiento de Tomcat se encuentra a cargo de miembros de Apache Software Fundation, a través del proyecto Jakarta, que a su vez, cuenta con la colaboración de desarrolladores independientes. El proyecto Tomcat Jakarta se ha venido desarrollado desde el año 1999 por iniciativa de James Duncan Davidson, quien se desempeñaba como trabajador de Sun Microsystems

y decidió donar el proyecto a Apache Software Foundation y se especializa en crear soluciones open source para la plataforma Java.

Entre otras características relevantes, se encuentra su carácter de software libre, distribuido bajo la Apache Licence 2.0, teniendo especificado en esta licencia la libertad de propósito en su uso, código abierto, entre otras. Así mismo, siendo desarrollado bajo código Java, Tomcat puede ejecutarse en cualquier sistema operativo en el que se tenga disponible Java virtual Machine (Máquina virtual de Java).

2.4 PLATAFORMAS DE LENGUAJES DE PROGRAMACIÓN

2.4.1 Lenguaje PHP (Hypertext Preprocessor)

Tanto para el servidor Sistemas como para el servidor Delfín, se ha hecho necesario implementar dos versiones del PHP, ya que se van a alojar sitios web que requieren de una versión anterior a la actual (estable) del lenguaje. Por tanto, se ha decidido de instalar la versión 5.2.6 para los sitios con requerimientos específicos de compatibilidad y una versión actual (versión 5.3.6) para los demás sitios sin requerimientos especiales respecto a éste lenguaje.

PHP es un lenguaje open source, creado especialmente para desarrollos de páginas web con contenido dinámico, el cual puede trabajarse incrustado en páginas HTML. Cuenta con una sintaxis similar a la de los lenguajes C, Java y Perl, con lo cual los programadores pueden aprenderlo de una manera eficiente. Con este lenguaje, se pueden diseñar páginas dinámicas, manejando conexiones a bases de datos, es multiplataforma y goza de un amplio soporte, por ser desarrollado en comunidad.

Es de aclarar que este lenguaje es utilizado principalmente para la interpretación del lado del servidor, con lo que el código fuente escrito en PHP es invisible al

navegador web y al cliente, ya que es el servidor el encargado de ejecutar el código y enviar el resultado HTML al navegador, lo cual agrega un factor de seguridad a los sitios web alojados desarrollados en dicho lenguaje.

Como datos históricos, es conocido que PHP proviene de un desarrollo anterior llamado PHP/FI, creado por Rasmus Lerdorf en 1995 como un conjunto de scripts escritos en Perl para control de acceso del curriculum online. Lerdorf llamó a ese conjunto de scripts 'Personal Home Page Tools'. Según se requería, fue añadiéndosele más funcionalidad utilizando lenguaje C, con lo que logró comunicarse con bases de datos y permitía a los usuarios desarrollar sencillas aplicaciones Web dinámicas. Posteriormente decidió liberar el código fuente de PHP/FI para que cualquiera pudiese utilizarlo, así como arreglar errores y mejorar el código fuente.

PHP/FI 2.0 se liberó oficialmente hasta Noviembre de 1997, después de seguir por tiempo prolongado en versión beta, pronto se liberaron las primeras versiones 3.0 y su desarrollo siguió haciéndose progresivamente. La versión actual es la PHP5, lanzada en Julio del 2004 después de un largo desarrollo y varios pre-releases, y contiene mejoras y nuevas opciones para el desarrollo orientado a objetos y desde el 14 de julio de 2011 fue lanzada la versión 5.4.0 (en versión Beta). La última versión estable liberada, es la 5.3.8 que contiene mejoras en seguridad y en gestión de bases de datos MySQL.

2.4.2 Máquina Virtual de Java (JVM-Java Virtual Machine)

La Máquina virtual de Java, está constituida por un conjunto de aplicaciones software, capaz de interpretar y ejecutar instrucciones de programas desarrollados en lenguaje Java.

Entre los software más importantes a instalar, que constituyen la máquina virtual Java, se encuentra el JRE (Java Runtime Environment), que es un conjunto de

utilidades que permite la ejecución de los programas Java; El JRE cumple con la tarea de intermediar entre el sistema operativo y Java. Para la ejecución de aplicaciones desarrolladas con lenguaje Java sólo es necesario tener instalado el JRE, mientras que para el desarrollo de aplicaciones Java, se debe contar con el entorno de desarrollo, denominado JDK (Java Development Kit), el cual incluye dentro de su paquete de desarrollo un compilador para Java.

Para ejecutarse una aplicación en una Máquina Virtual de Java, el código de programa debe compilarse de acuerdo al formato binario portable estandarizado, que se generan normalmente en forma de ficheros con extensión *".class"*. Es de saberse que un programa puede componerse de múltiples clases, en cuyo caso cada clase tendrá asociada su propio archivo *.class*. Para facilitar la distribución de aplicaciones, los archivos de clase pueden empaquetarse juntos, en un archivo con formato *.jar*. Esta idea apareció en la época de los primeros applets de Java montados en páginas web. Estas aplicaciones podían descargar los archivos de clase que necesitaban en tiempo de ejecución, lo que suponía una sobrecarga considerable para la red en una época donde la velocidad suponía un problema; entonces, lo que se logra con el empaquetado, es evitar la sobrecarga por la continua apertura y cierre de conexiones para cada uno de los fragmentos necesarios, teniendo el programa completo (incluyendo sus librerías) en un solo fichero ejecutable.

Java fue creado como una herramienta de programación para utilizarse en un proyecto de *set-top-box* (decodificador de señal digital) en una pequeña operación denominada the Green Project en Sun Microsystems en el año de 1991. El equipo (Green Team), compuesto por trece personas y dirigido por James Gosling, trabajando conjuntamente en Sand Hill Road en Menlo Park para su desarrollo.

El lenguaje se llamó inicialmente Oak (por un roble que había fuera de la oficina de Gosling), luego pasó a denominarse Green tras descubrir que Oak era ya una

marca de adaptadores de tarjetas gráficas, finalmente tomó el nombre actual de Java. En abril de 2009 Oracle adquirió Sun Microsystems lo cual hizo que Java pasara al poder de Oracle, generando temor en la comunidad ante la posible mercantilización del lenguaje. Por ahora, Oracle ha seguido manteniendo Java bajo licencia libre GPL, siendo las versiones posteriores a la 6.0 lasque estarán bajo su control.

En los servidores Sistemas y Delfín se ha instalado la Máquina Virtual de Java, en su versión Java6, para soportar en conjunto al servidor Tomcat 6 a los sitios y aplicativos alojados que requieran del entorno de ejecución Java, tales como sitios web desarrollados en JSP (Java Server Pages) o aquellas páginas con contenidos empaquetados de Java (.jar) o servlets, brindando un espacio propicio para hospedar contenido Java que se desarrolle en la Escuela de Ingeniería de Sistemas y se aloje en dichos servidores.

2.5 GESTORES DE BASES DE DATOS

2.5.1 MySQL

Se ha instalado como gestor de base de datos el MySql en su versión actual (MySql 5), por ser un sistema estable, seguro y de fácil administración, además es de libre distribución, ya que cuenta con licencia GPL; aunque ya se encuentran versiones enterprise disponibles y su desarrollo actualmente es patrocinado por la empresa privada MySql AB, cuyo propietario es Oracle, que posee el copyright de la mayor parte del código, es la encargada del desarrollo, generar la documentación y dar soporte.

Entre las características más relevantes se encuentran:

- Escrito en C y en C++
- Probado con un amplio rango de compiladores diferentes

- Funciona en diferentes plataformas. Entre las más importantes están GNU/Linux, Mac, Windows (Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Vista, Windows 7 y Windows Server), Solaris, FreeBSD, entre otras.
- Proporciona sistemas de almacenamiento transaccional y no transaccional.
- Soporte completo para Unicode.
- Transacciones con motores de almacenamiento InnoDB, BDB y Cluster. Permite realizar puntos de recuperación (savepoints) con InnoDB.
- El servidor está disponible como un programa separado para usar en un entorno de red cliente/servidor. También está disponible como biblioteca y puede ser enlazado en aplicaciones autónomas.
- Un sistema de privilegios y contraseñas que es muy flexible y seguro, y que permite verificación basada en el host. Las contraseñas son seguras porque todo el tráfico de contraseñas está cifrado cuando se conecta con un servidor.
- Soporta gran cantidad de datos. MySQL Server tiene bases de datos de hasta 50 millones de registros.
- La conexión con MySQL puede realizarse desde cualquier plataforma utilizando sockets TCP/IP. En sistemas Windows de la familia NT (NT, 2000, XP, o 2003). En sistemas Unix, los clientes pueden conectar usando ficheros socket Unix.
- Soporta variados conjuntos de caracteres, incluyendo latin1 (ISO-8859-1), german, big5, ujis, y más. Por ejemplo, los caracteres escandinavos 'â', 'ä' y 'ö' están permitidos en nombres de tablas y columnas. Soporta además Unicode.
- Todos los datos se guardan en el conjunto de caracteres elegido.

MySql inició como parte de un proyecto de la empresa MySQL AB, fundada en 1995, y parte de la idea básica de SQL (Structured Query Language),

comercializado desde 1981 por IBM. El objetivo perseguido por lo creadores de MySql consistía en que su proyecto cumpliera con el estándar SQL, pero sin sacrificar velocidad, fiabilidad o usabilidad.

Michael "Monty" Widenius, quien fue uno de los fundadores de MySql AB , trató inicialmente usar mSQL para conectar las tablas usando piezas de código de bajo nivel, sin embargo, éste no era rápido ni flexibles para tal propósito. Esto lo llevó a crear una API SQL denominada MySQL para bases de datos muy similar a la de mSQL pero más portable. En el año 2008 Sun Microsystems adquirió la empresa, lo cual se integraron los productos de MySql AB con los de esta compañía y posteriormente Sun Microsystems fue adquirida por Oracle; aunque el desarrollo de MySql sigue estado a cargo de MySql AB.

2.6 GESTORES DE CORREOS

2.6.1 Postfix

Para dar soporte de envío de correo a los sitios alojados en ambos servidores, en especial a las Aulas Virtuales de MeiWeb y Moodle, se ha optado por la instalación de Postfix, que es un servidor de correos MTA (Mail Transport Agent), rápido, fácil de administrar, seguro y con buen soporte y documentación en su sitio web. Es un software de open source de libre distribución.

Entre las características más relevantes de Postfix se encuentra:

- Soporte para TLS (Transport Layer Security).
- Soporte para distintas bases de datos LDAP, MySQL, PostgreSQL.
- Soporte para mbox, maildir y dominios virtuales.
- SMTP-AUTH, SASL (Simple Authentication and Security Layer) y reescritura de dirección, para redirección segura de los paquetes.
- Soporte para filtrado de correos *“Milter”* (Mail Filter)
- Capacidad de manejar altos volúmenes de correo.

Otra característica relevante de Postfix, es que cuenta con un esquema de seguridad contra el uso inadecuado (spam, relay, etc.), debido a que soporta directamente (sin modificaciones suplementarias) listas negras y que es complicado configurarlo como relay abierto (vulnerablilidad a ataques de hackers y spammers). Además, se puede instalar Postfix de forma que corra en modo chroot, lo que le confiere a su operativa más seguridad.

Postfix se creó como alternativa libre de MTA libre, en la cual se buscaba un servidor rápido, de fácil administración y seguro; es de hecho, un MTA que se usa por defecto en muchos sistemas operativos derivados de UNIX, entre ellos, GNU/Linux y se distribuye bajo Licencia Pública IBM v.1.0, que es una licencia de software libre. Fue desarrollado por Wietse Venema durante una estancia en el Centro de Investigación Thomas J. Watson de IBM y fue conocido con el nombre de *"VMailer"* e *"IBM Secure Mailer"*, siendo distribuido al gran público por primera vez a mediados de 1999.

2.6.2 Cyrus IMAP

Para la creación de cuentas de correo locales y almacenamiento de correo electrónico, se ha utilizado el servidor Cyrus IMAP, que permite administrar el almacenamiento de correo de forma organizada, al crear para cada mensaje su propio fichero. Es un software de libre distribución, que cuenta con licencia BSD (Berkeley Software Distribution), que es una licencia que difiere de la GPL (General Public License), en que BSD permite el uso del código fuente en software no libre.

Cyrus IMAP, es un servidor que proporciona acceso a correo electrónico personal a través del protocolo IMAP (Internet Message Access Protocol). Es además un sistema de correo electrónico organizacional escalable diseñado para su uso en entornos desde pequeñas a grandes organizaciones, utilizando tecnologías basadas en estándares.

Entre las características principales de Cyrus IMAP, es que cuenta con un diseño de buzón de base de datos privado, ofreciendo ventajas de servidores de gran tamaño en la eficiencia, la escalabilidad y de administración. Permite conexiones múltiples de lectura/escritura al mismo buzón. El servidor soporta las listas de control de acceso en los buzones y cuotas de almacenamiento para los buzones de los usuarios.

Es fundamental mencionar que Cyrus ofrece entre sus configuraciones adicionales, un paquete llamado Cyrus SASL, con el cual se puede realizar autenticación mediante SASL (Simple Authentication and Security Layer), que provee la infraestructura para autenticación y autorización en protocolos de Internet, que ha sido estandarizado por la IETF (Internet Engineering Task Force). Es usado para manejar las peticiones de autenticación de los clientes, para ello, el protocolo incluye un comando para identificar y autenticar un usuario contra un servidor. La librería SASL de Cyrus también usa la librería OpenSSL para cifrar los datos.

2.6.3 GNU Mailman

Para la organización de correo entrante y de listas de listas de correos electrónicos para los usuarios del servidor de correos, se ha instalado el paquete GNU Mailman, que es un software libre que le permite administrar listas de correo electrónico a los usuarios, con soporte para un rango amplio de tipos de listas de correo electrónico, tales como listas de discusión general y listas de sólo anuncios. Posee características extensivas que lo hacen bueno para listas de suscriptores, tales como facilidad en la suscripción y cancelar una suscripción, opciones de privacidad y la capacidad de detener temporalmente la recepción de los envíos a la lista.

Así mismo, tiene muchas características que lo hacen atractivo para usuarios en su administración de listas y sitio, tales como, detección de rebote de correos y

manejo automático de direcciones de rebote, integración con filtros de correo no deseado, realización cambios en algunas de sus opciones de entrega a nivel global para todas las listas en un sitio, incluyendo su contraseña, el estado de entrega, nombre real, entre otras características.

2.6.4 SquirrelMail

Para el acceso vía web a las bandejas de correos de los usuarios del servidor de correos, se optó por la instalación de SquirrelMail en su versión 1.4 que es un paquete de correo web basado en estándares, está escrito en PHP y es de libre distribución ya que cuenta con licencia GNU de software libre.

SquirrelMail es una aplicación que permite el fácil uso del correo electrónico para los usuarios, a su vez tiene requisitos mínimos para su instalación, facilitando su configuración y gestión a los administradores. Además, incluye una función de soporte de PHP puro para los protocolos IMAP (Internet Message Access Protocol), y SMTP (Simple Mail Transfer Protocol), su desarrollo está basado en el estándar HTML 4.0, lo cual lo hace compatible con la mayoría de los navegadores web y tiene toda la funcionalidad que se quiere de un cliente de correo electrónico, incluyendo un fuerte apoyo MIME (Multipurpose Internet Mail Extensions), libreta de direcciones y manipulación de carpetas.

2.7 CLÚSTER DE ALTA DISPONIBILIDAD

2.7.1 Modo de Operación

Los clúster de alta disponibilidad, son agrupaciones de dos o más servidores que trabajan con sistemas de almacenamiento de datos y servicios compartidos, lo cual implica que los equipos que pertenecen al clúster, deben estar en permanente comunicación para reaccionar ante cualquier evento imprevisto. Si se llega a presentar algún tipo de fallo, ya sea de hardware o de los servicios de alguna de las máquinas que forman parte del clúster, el software de alta

disponibilidad actúa inmediatamente para promover los servicios y los datos a alguno de otros equipos que hacen parte del clúster.

En el siguiente esquema se aprecia un modelo de clúster de alta disponibilidad creado con dos nodos (dos equipos servidores), en el que se aprecia el funcionamiento básico del clúster.

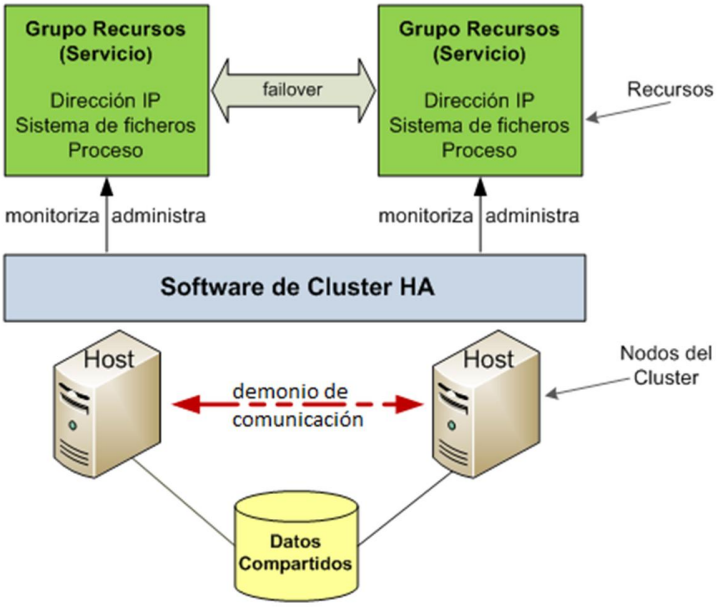

Figura 3 Clúster de Alta Disponibilidad de dos nodos. Fuente http://www.lintips.com/

En la figura se observan dos nodos (Hosts), éstos comparten los datos que se encuentran dentro de un disco o partición específico de sincronización, que deben tener el mismo tamaño y características, para que estos datos estén sincronizados constantemente y correctamente. Además de datos, se puede configurar la disponibilidad de recursos (servicios) instalados en ambos nodos. Los datos y los recursos se sincronizan a través del software de gestión del Clúster y del uso de un demonio de comunicación que pasa información constantemente entre los nodos del clúster acerca del estado de los servicios y recursos compartidos.

La infraestructura base del clúster se puede implementar de diferentes maneras y con diferente software según sea el propósito o la disposición requerida de los

recursos. A continuación se muestra algunas de las infraestructuras más utilizadas para el diseño de clúster de alta disponibilidad utilizando las herramientas DRBD, Pacemaker, Corosync/OpenAIS, de las cuales se detalla su funcionalidad en la sección 2.7.2 de este libro.

- **Activo/Pasivo:** Uno de los dos nodos del clúster tiene activos los servicios y los sistemas de archivos compartidos, el otro los tiene en espera, en caso de fallo.

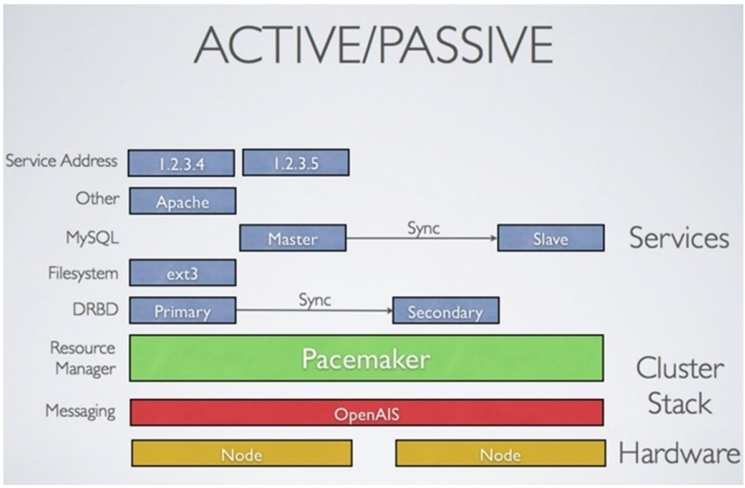

Figura 4 Esquema de clúster con infraestructura Activo/Pasivo. Fuente http://www.clusterlabs.org/

- **N+1:** Esta infraestructura puede contar con más de dos nodos. Cuenta con varios nodos Activos/Pasivos, teniendo un nodo de backup común compartido, lo cual ayuda a reducir los costos de hardware por equipo.

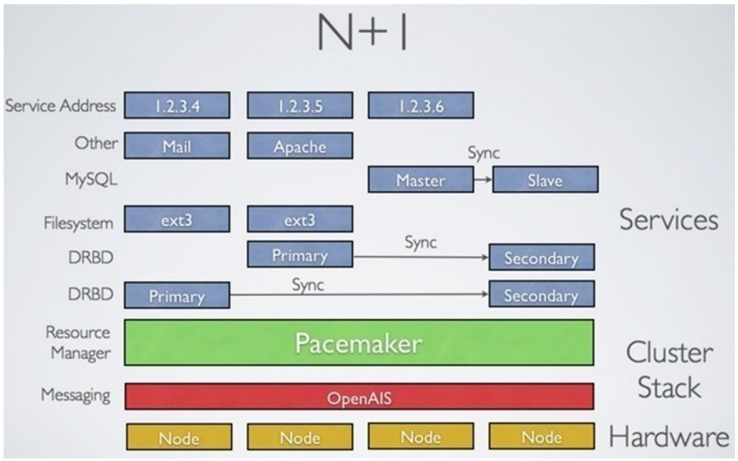

Figura 5 Esquema de clúster con infraestructura N+1. Fuente http://www.clusterlabs.org/

- **N a N:** Todos los nodos del clúster se encuentran en estado Activo, lo cual permite que todos los nodos puedan ser potencialmente utilizados en caso de fallos, corriendo simultáneamente múltiples copias de los servicios, balanceando de esta forma la carga de trabajo entre los diferentes nodos.

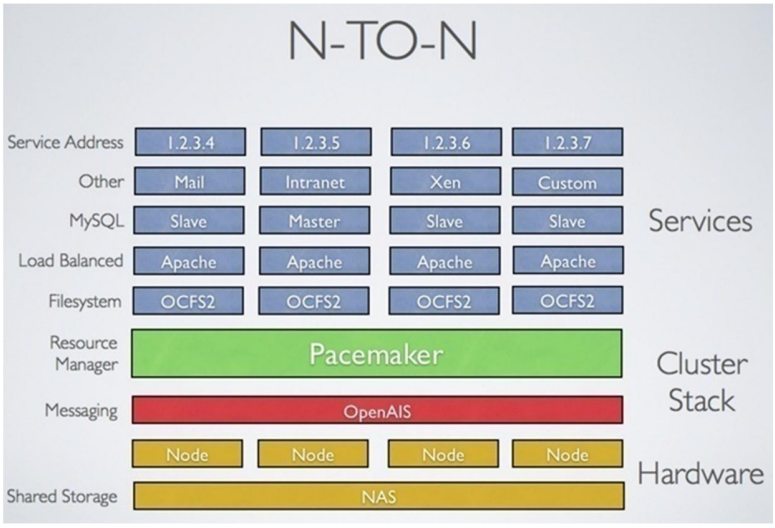

Figura 6 Esquema de clúster con infraestructura N a N. Fuente http://www.clusterlabs.org/

- **Split-site Clúster:** Un clúster de estas características tiene compartido el almacenamiento de datos por red en los diferentes nodos del clúster, mientras que los servicios se encuentran activos en uno o más nodos y los omite en los demás nodos.

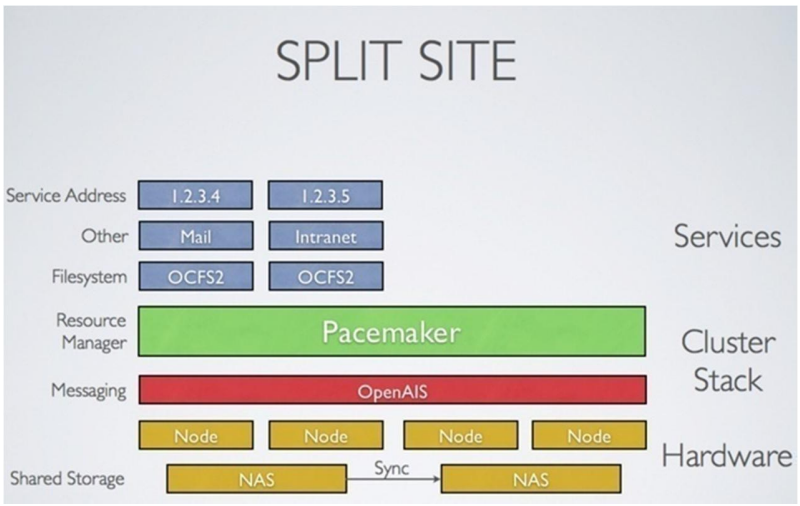

Figura 7 Esquema de clúster con infraestructura Split-site. Fuente http://www.clusterlabs.org/

2.7.2 Software para la Alta Disponibilidad

Para la creación del clúster de alta disponibilidad con los dos servidores (Sistemas y Delfín), se han utilizado las herramientas de software libres DRBD, Pacemaker, Corosync/OpenAIS y se decidió utilizar la infraestructura de Clúster Activo/Pasivo para su montaje.

Antecediendo la instalación de todas las herramientas nombradas, se realizó todo un proceso investigativo acerca de las herramientas disponibles para alta disponibilidad, encontrando variadas alternativas de software; finalmente, se optó por el software mencionado por diversos factores, entre los cuales se encuentra:

- Todas las herramientas software implementadas son de carácter libre.
- Poseen documentación completa y soporte actualizado.
- Cuentan con buenas características de seguridad.
- Son adaptables a diferentes esquemas de funcionamiento según sea requerido.
- Trabajan muy bien como conjunto, brindando una infraestructura de clúster de eficiente gestión.

2.7.2.1 DRBD (Distributed Replicated Block Device)

Es un software que permite la creación de sistemas de almacenamiento distribuido y opera en sistemas GNU/Linux. Esto se hace mediante la duplicación de un dispositivo (disco, partición, volumen lógico, etc.) a través de una red asignada. DRBD puede entenderse como una red basada en RAID-1 (copia exacta o espejo de un conjunto de datos en dos o más discos).

En DRBD, todos los recursos tienen un rol, el cual puede ser Primario o Secundario:

- Un dispositivo DRBD con rol primario se puede utilizar sin restricciones de lectura y escritura. Se puede utilizar para crear y montar sistemas de

archivos sin formato, E/S directa al dispositivo de bloques, ext 3, ext 4, volúmenes lógicos, entre otros.

- Un dispositivo DRBD con rol secundario recibe todas las actualizaciones del dispositivo del nodo del mismo nivel, pero contrariamente no permite el acceso completo. No puede ser utilizado por las aplicaciones, ni para leer ni escribir. La razón para no permitir el acceso, incluso de sólo lectura en el dispositivo, es la necesidad de mantener la coherencia de caché, lo cual sería imposible si un recurso secundario se pusiera a disposición de cualquier forma.

Así mismo, DRBD soporta tres modos distintos de replicación, lo cual se detalla en tres protocolos de sincronización:

- **Protocolo A:** Protocolo de replicación asíncrona. Las operaciones locales de escritura en el nodo principal se consideran finalizadas tan pronto como la escritura en disco local ha terminado y el paquete de replicación se ha colocado en el buffer de envío local TCP. En el caso de un fail-over forzado, puede ocurrir pérdida de datos. Los datos en el nodo de espera son consistentes después del fail-over, sin embargo, las actualizaciones más recientes realizadas antes del accidente se pueden perder. El Protocolo A es el más utilizado en los escenarios de replicación de larga distancia. Cuando se utiliza en combinación con DRBD Proxy, tiene una solución de recuperación eficaz ante desastres.
- **Protocolo B:** Protocolo de replicación de memoria síncrona (semi-síncrona). Las operaciones locales de escritura en el nodo principal se consideran finalizadas tan pronto como la escritura del disco local se ha producido y el paquete de replicación ha alcanzado el nodo par (peer node). Normalmente, los datos no escritos se pierden en caso de fail-over forzado. Sin embargo, en caso de fallo de alimentación simultánea en ambos nodos y destrucción simultánea e irreversible del sistema de almacenamiento de

datos principal, las acciones de escritura completadas en el nodo primario se pueden perder.

- **Protocolo C:** Protocolo de replicación síncrona. Las operaciones locales escritura en el nodo principal se considera completas sólo después de que tanto a nivel local como remoto, la escritura se han confirmado. Como resultado, al perder un solo nodo se garantiza que no producirá ninguna pérdida de datos. La pérdida de datos es inevitable, por supuesto, si ambos nodos (o sus subsistemas de almacenamiento) son destruidos irreversiblemente al mismo tiempo.

La sincronización es diferente a la replicación de dispositivo. Mientras que la replicación se produce en todo evento de escritura para un recurso en rol principal, la sincronización es desacoplada desde la entrada de escritura, afectando el dispositivo de almacenamiento en su totalidad.

2.7.2.2 Corosync/OpenAIS

OpenAis, es un software que provee una interfaz de clúster basada en estándares, que cuenta con licencia Open Source, para dar servicios de Alta de Disponibilidad AIS (Application Interface Specification). La AIS es una API (Application Programming Interface) de software, que sirve para desarrollar aplicaciones que mantienen el servicio durante las fallas. El software OpenAIS actualmente se encuentra construido para funcionar como complemento al motor de clúster Corosync.

Corosync es un producto derivado del proyecto OpenAis, el cual se creó para dar apoyo a la infraestructura API del OpenAis en un principio, pero luego fue tomando su forma actual como motor de clúster. Los desarrolladores de Corosync, han reutilizado aproximadamente el 80% del código de OpenAis en la ejecución Corosync. El 20% restante se centra principalmente en torno a las APIs que están fuera del alcance de la misión de Corosync.

Corosync, es un Sistema de Comunicación de Grupo, con características adicionales para la implementación de alta disponibilidad dentro de las aplicaciones que se dispongan dentro del Clúster. Este provee las siguientes cuatro características a través de una Interfaz de Programación de Aplicaciones en lenguaje C:

- Un modelo de comunicación de grupo de procesos cerrado, con todas las garantías de sincronía virtual para la creación de máquinas con estado replicado.
- Un Administrador Simple de Disponibilidad, que reinicia los proceso de las aplicaciones cuando tienen fallos.
- Una base de datos con la configuración y las estadísticas en memoria, que proporcionan la capacidad para establecer, recuperar y recibir notificaciones de cambio de la información.
- Un sistema de quórum (agrupación de aplicaciones) que notifica a cada una de las aplicaciones del grupo cuando el quórum es logrado o cuando se pierde.

2.7.2.3 Pacemaker

Pacemaker es un software gestor de servicios (recursos) de clúster para plataformas Linux. Logra la máxima disponibilidad de sus servicios de clúster mediante la detección y la recuperación de los nodos y los fallos a nivel de recursos, haciendo uso de la mensajería y capacidades de composición proporcionada por la infraestructura de clúster que se prefiera (ya sea Corosync/OpenAIS o Heartbeat).

Pacemaker puede hacer esta labor para clústeres de prácticamente cualquier tamaño y viene con un modelo de dependencia potente que permite que al administrador expresar con precisión las relaciones (tanto orden y la ubicación) entre los recursos del clúster. Prácticamente todo lo que puede se puede hacer

por medio de scripts para alta disponibilidad, puede ser administrado como parte de un grupo en la configuración de Pacemaker.

Por otra parte, Pacemaker no es derivado de Heartbeat, ya que son desarrollos separados y sus codificaciones pertenecen a proyectos independientes. El Pacemaker es una continuación de la CRM (también conocido como administrador de recursos v2) que fue desarrollado originalmente para Heartbeat, pero se convirtió en un proyecto aparte.

Algunas de las características relevantes de Pacemaker son:

- Detección y recuperación de nodo y los fallos a nivel de servicio (recursos).
- Almacenamiento agnóstica, sin necesidad de almacenamiento compartido.
- Recurso agnóstico, algo que puede ser escrito pueden ser agrupado.
- Soporte de clústeres grandes y pequeños.
- Soporte para prácticamente cualquier configuración de redundancia entre ellas: Activo / activo, activo / pasivo, N + 1, N + M, N - 1 y N a N.
- Opcionalmente garantiza la integridad de los datos con STONITH (Shoot The Other Node In The Head). Es una técnica que permite asegurar que un servidor que esté en un estado de fallo no interfiera con el funcionamiento del clúster.
- La capacidad de especificar todo el clúster en cuanto a orden, colocación y anti-colocación de los servicios.
- Tipos de recursos avanzados.
- Soporte de servicios que necesitan estar activos en varios nodos.
- Soporte de servicios con múltiples modos (por ejemplo, maestro / esclavo, primario / secundario).
- Unificado, configurable mediante scripts, clúster por comandos Shell.

En general, en caso de un fallo, el administrador de recursos Pacemaker, es el que se encarga de forma automática del inicio de la recuperación y se asegura de que su solicitud está disponible en una de las máquinas restantes que conforman el clúster, esto lográndose con el apoyo de las demás herramientas software para la alta disponibilidad descritas anteriormente.

2.7.3 Pruebas de Clúster

Todo el software antes mencionado, antes de ser instalado en los equipos, fue sometido a pruebas controladas, con las cuales se buscaba no afectar, en ningún caso, la funcionalidad de los equipos en la prestación de servicios a los usuarios, para de esta forma, evitarles que su trabajo cotidiano se viera afectado por dichas pruebas, ya que dentro de las pruebas de clúster, se involucran los servicios de Apache y de base de datos MySQL, fundamentales en el funcionamiento de los servicios web.

Ante esto, el proceso de pruebas se inició con la creación de dos máquinas virtuales en computadores personales, apoyados con el software de virtualización VirtualBox; éstas máquinas fueron configuradas con características similares a las de los equipos reales, en cuanto al Sistema Operativo Debian de 64 bits, software instalado y esquema de particionado, aunque este último en una escala considerablemente menor de tamaño, debido a las limitaciones de disco, memoria RAM y capacidad de procesamiento de los ordenadores utilizados. En las pruebas se buscaba evaluar el comportamiento general del software de alta disponibilidad y su trabajo en relación a los servicios de Apache, MySQL y los datos compartidos. Igualmente, se simularon caídas de servicios y el paso de recursos del nodo activo al pasivo, forzando el cambios de roles, es decir, el activo pasa a tener rol pasivo y viceversa.

En el clúster creado con las máquinas virtuales también se realizaron pruebas de simulación del entorno de producción de los sitios web, simulando caídas de los

nodos del clúster, manejo de datos, ingreso de nuevos datos y en general, el comportamiento del los servicios web en función de la estructura funcional del clúster implementado. A continuación, se observa el comportamiento normal del clúster montado en las máquinas virtuales de prueba.

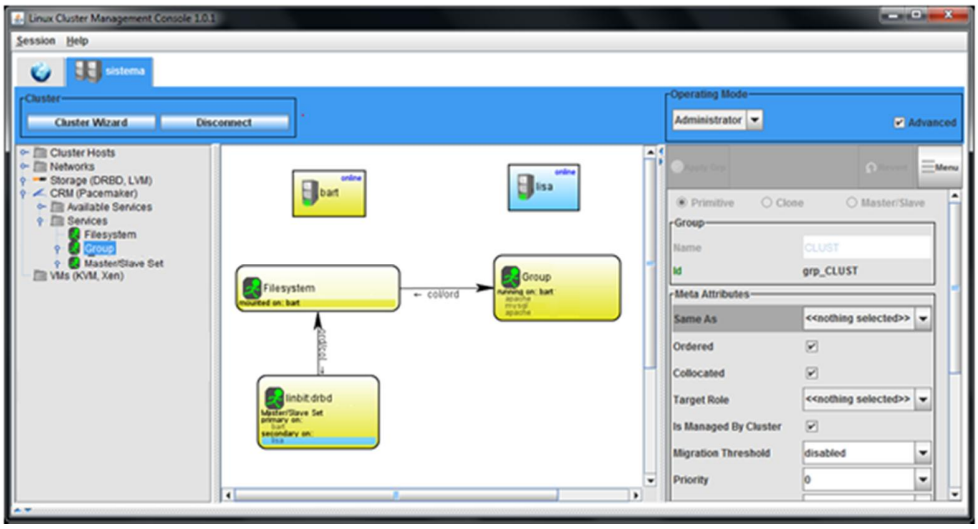

Figura 8 Clúster Activo/Pasivo de máquinas virtuales de prueba

La anterior figura, muestra el esquema de clúster gestionado por medio del GUI Linux Cluster Management Console (LCMC), del cual se habla con mayor detalle y de su manejo en el apartado 3.7 (Administración del clúster). En éste se observan ambos nodos, nombrados Bart y Lisa, actuando estos con el rol activo y pasivo respectivamente y en la parte inferior se muestra la configuración del clúster, que incluye los recursos gestionados para alta disponibilidad (Apache y MySQL), los sistemas de archivos que trabajan con DRBD y el rol asignado para cada nodo.

En las pruebas de simulación de fallos, al simular la caída del nodo principal (llamado Bart), ocurría un evento en el cual se realizaba el relevo pero se generaba una condición de error debido a la pérdida de comunicación entre los nodos del clúster. En la siguiente imagen, se observa la caída del nodo principal Bart, graficado con una barra lateral color rojo. La corrección de tal estado debe

realizarse manualmente y tal proceso se encuentra en el manual interno de administración cuyo contenido es privado para la gestión exclusiva de los equipos.

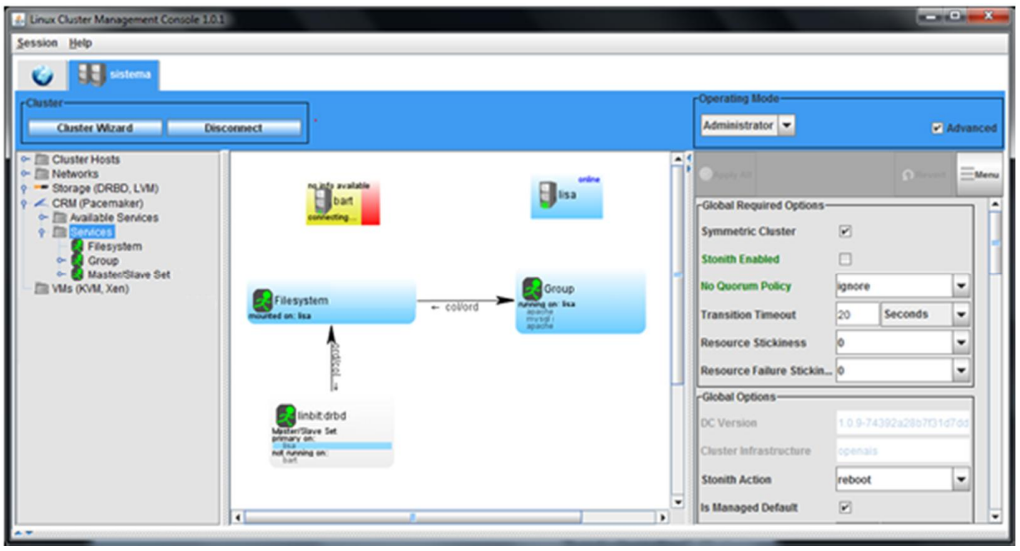

Figura 9 Caída del nodo activo y relevo al segundo nodo

Igualmente, al simular la caída del nodo Lisa, se generó una condición de error por la pérdida de comunicación entre los nodos. En la figura 10, se observa tal evento desde la interfaz del LCMC. La franja roja desaparece, una vez finalizado el proceso de sincronización de los discos.

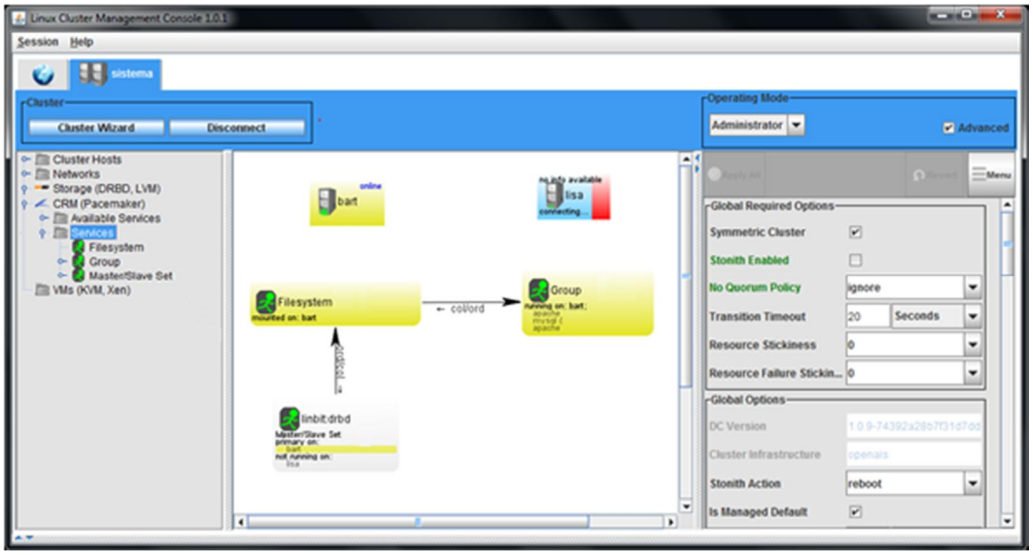

Figura 10 Caída del nodo pasivo

A continuación se muestra algunos datos tomados durante el proceso de pruebas en las máquinas virtuales:

No. Toma	Tiempo de Promoción (seg)
1	8,63
2	10,55
3	10,9
4	10,4
5	11,54
6	19,57
7	9,33
8	9,36
9	27,33
10	9,48
11	18,77
12	8,93
13	21,86
14	29,33
15	33,63
Media	15,974
Desviación	8,2218277

Tabla 1Muestra de tiempo de promoción (Máquina virtual)

No. Toma	Tiempo de Estabilización (seg)
1	11,61
2	11,7
3	15,2
4	11,08
5	40,46
6	9,75
7	15,26
8	13,52
9	15,85
10	14,45
11	15,78
12	19,05
13	14,75
14	15,01
15	17,6
Media	16,0713333
Desviación	6,94484352

Tabla 2 Muestra de tiempo de Estabilización (Máquina virtual)

Como se observa en las dos tablas anteriores, se tomaron 15 datos en cada muestra, donde se resalta el funcionamiento del clúster para promover un nodo de secundario a primario, y el tiempo de estabilización de dicho clúster, es decir, el tiempo empleado en la incorporación del nodo en el clúster y la puesta en marcha de servicios nuevamente. La caída de la red en uno de los nodos, fue el método de medición de estas funciones del clúster.

Antes de presentar el análisis de la muestra, es pertinente decir que el error implícito en cada dato tomado, viene dado por los siguientes factores considerados como error:

- La velocidad de respuesta del otro nodo a través del canal de comunicación.
- El instrumento de medición.
- La velocidad a la hora de finalizar o empezar la toma de las medidas.

Al final de dichas pruebas, se pudo tomar nuevas decisiones y realizar ajustes, para que de esta manera se dieran condiciones más óptimas en el proceso de prueba en los equipos servidores. En esta etapa se observó:

- Una vez establecida la configuración de comunicación en los diferentes nodos que integran el clúster, los equipos se reconocen constantemente por red para monitorearse conjuntamente y reaccionar ante cualquier anomalía.
- La media de los datos, es aproximadamente de 16 segundos para la promoción y la estabilización, se consideran apropiados, ya que es un tiempo relativamente pequeño para que se haga lo cometido en el clúster de alta disponibilidad.
- La desviación en los tiempos tomados en ambos escenarios se consideran aceptables, a pesar, de que existen mediciones atípicas, pero se pueden considerar factores tanto externos como internos a la hora de evaluar dichas tomas, como por ejemplo el error en la medida.
- Los datos compartidos que trabajan bajo DRBD, se replican en modo espejo de un nodo a otro, estando habilitados para su uso únicamente en el nodo activo.
- El anterior proceso se realiza automática y constantemente.
- El monitoreo del clúster se hará por medio del software Linux Cluster Management Console (LCMC).
- El cambio de rol también se puede gestionar para realizarse de forma no automática.

Realizadas las pruebas en máquinas virtuales y realizadas las observaciones correspondientes, se llevó a cabo las pruebas de funcionando de los equipos Sistemas y Delfín, trabajando como un clúster de alta disponibilidad, en el cual se puso a prueba los servicios de Apache, bases de datos MySQL, y volúmenes lógicos con datos compartidos. De igual manera se probaron los sitios web, tal y como se hizo en las pruebas de máquinas virtuales.

En las primeras pruebas físicas, se optó por no ocupar los dominios sistemas.uis.edu.co ni delfin.uis.edu.co, para que los servicios web no se vieran afectados por dichas pruebas, estando éstos alojados en los equipos servidores antiguos; por lo que en esta fase, se hicieron las pruebas en un ambiente de red interna, asignando a cada equipo una dirección IP privada.

No. Toma	Tiempo de Promoción (seg)
1	6,42
2	9,67
3	12,47
4	7,91
5	8,59
6	6,51
7	13,83
8	12,41
9	10,35
10	7,34
11	20,67
12	18,93
13	23,55
14	14,48
15	27,26
Media	13,3593333
Desviación	6,27765929

Tabla 3 Muestra de tiempo de promoción (Máquina Real)

No. Toma	Tiempo de Estabilización (seg)
1	8,47
2	10,18
3	14,06
4	9,5
5	12,37
6	15,24
7	11,19
8	10,23
9	16,96
10	15,74
11	20,91
12	21,62
13	18,03
14	25,71
15	19,17
Media	15,292
Desviación	4,92873912

Tabla 4 Muestra de tiempo de Estabilización (Máquina Real)

Como se observa en las tablas anteriores, se realizaron las mismas pruebas que en las máquinas virtuales, observando el comportamiento del clúster. En esta etapa, no se presentaron mayores variaciones en la forma de operación del clúster respecto a las pruebas de las máquinas virtuales; los cambios visibles fueron a nivel de la cantidad de tiempo empleado en cada una de las tomas, teniendo en el tiempo de promoción de nodos de primario a secundario una media de aproximadamente 13 segundos y para la estabilización del clúster una media de 15 segundos aproximadamente. A partir de estas pruebas se tomaron las siguientes decisiones:

- Trabajar la comunicación del clúster por red local con interfaces de red independientes a las interfaces configuradas para los dominios sistemas.uis.edu.co y delfin.uis.edu.co, por efectos de seguridad e integridad del clúster principalmente.
- Para la promoción de roles en los nodos del clúster, cuando se requiera reorganización de éstos, los servicios no deben estar activos, por tanto, tal actividad se debe realizar en un momento adecuado del día.

Finalmente, se hizo las pruebas con los servicios migrados y en el ambiente real de producción, las configuraciones mencionadas, pero manteniendo las interfaces de red del clúster independientes a los dominios sistemas.uis.edu.co y delfin.uis.edu.co, pues en casos de fallo de red o del servidor DNS de la Universidad, la comunicación del clúster no se vería afectada. Estas pruebas no tuvieron ninguna variación, el software de alta disponibilidad y los recursos manejados por éste mantienen un comportamiento estable, por lo que se ha dejado trabajando sin imprevistos y su monitoreo se realiza periódicamente a través de los Logs del sistema y del software de administración Cluster Management Console, anteriormente mencionado.

3. GESTIÓN ADMINISTRATIVA

Con la instalación y configuración de los diferentes paquetes software en los servidores, la labor de administración se centra en la creación de esquemas para la gestión de la seguridad, de los usuarios y grupos, de los recursos, automatización de tareas administrativas, mantenimiento y administración del clúster de alta disponibilidad, por medio de un modelo administrativo en el que se contemple aquellas áreas en que repercutan en la prestación de los servicios.

3.1 GESTIÓN DE LA SEGURIDAD

La configuración de seguridad de los servidores, conforma una de las principales funciones de la gestión administrativa, ya que a partir de esta puede mitigarse, y por consiguiente neutralizarse, los diversos ataques que se puedan presentar cotidianamente. La labor de seguridad es entendida como un proceso continuo, que involucra no sólo la creación del esquema de seguridad, sino también aspectos como el monitoreo administrativo continuo del sistema para visualizar los puntos más vulnerables y el fortalecimiento de estos, con el fin de reducir las oportunidades de ataque y por consiguiente, hacer que la probabilidad de vulnerar el sistema sea menor.

3.1.1 Aseguramiento del Hardware

El proceso de aseguramiento del hardware consiste en mitigar los riesgos y amenazas frente a ingreso no autorizado al lugar en el que se encuentran ubicados los equipos informáticos. Tener regulado el acceso físico a los equipos es tan fundamental como el aseguramiento del sistema mismo. Esto se logra por medio de políticas de seguridad internas y control de acceso físico, no obstante si se lograse acceso físico a los servidores por parte de personal no autorizado se deben tomar otras medidas preventivas.

Una de estas acciones a tomar, es el aseguramiento por contraseña del BIOS (Basic Input/Output System), para que las modificaciones en el esquema base de operación del hardware sólo pueda ser alterado por usuarios plenamente identificados, en este caso, el administrador. De igual forma, el gestor de arranque del sistema (Boot) se ha asegurado y configurado, a fin de que sólo pueda ser modificado por los administradores en caso tal que se requiera hacerlo, mitigando de esta manera la probabilidad de daños en caso que se llegase a vulnerar la seguridad del acceso físico a los equipos. Con estas políticas de seguridad al acceso físico es posible neutralizar una gran cantidad de amenazas que se presenten por dicho aspecto, teniendo de esta forma menor probabilidad de perder el control del sistema por ataques físicos y del hardware en general.

3.1.2 Aseguramiento de Sistema Operativo

Entre los aspectos básicos a considerar para el aseguramiento del sistema, hay que tener en cuenta el sistema operativo implantado en los servidores. Es de resaltar que ningún sistema operativo que se comunica en una red o que sea visible en internet, es completamente seguro.

La forma más efectiva de asegurar el sistema operativo es mediante la instalación de actualizaciones de seguridad, estas actualizaciones pueden varias de una distribución a otra. En el caso de Debian GNU/Linux, las actualizaciones se publican en el sitio web oficial de Debian en el apartado de seguridad (http://www.debian.org/security/). Para hacer estas publicaciones, existe un equipo de seguridad dentro de la comunidad de desarrolladores de Debian, que reciben notificaciones sobre incidentes con el sistema, y luego hacen la evaluación correspondiente para trabajar en este.

Luego, prueban la solución y la compilan para todas las arquitecturas para las que se ofrezca soporte y se publica en aviso de seguridad y el paquete en el servidor de descargas. El soporte proporcionado por los desarrolladores y el equipo de

seguridad de Debian, en cuanto a la corrección de vulnerabilidades en el sistema, hacen relativamente más confiable el sistema ante amenazas que se puedan presentar.

En la labor de administración de los servidores, se ha optado por hacer revisión periódica de las actualizaciones de seguridad disponibles para evaluar las posibilidades de instalación, qué parte del sistema asegura y las implicaciones de su instalación; esto se hace con el fin de prevenir que otras partes del sistema se afecten negativamente tras su instalación, es decir, el impacto de la actualización en el funcionamiento del sistema, a fin de no provocar fallos en la prestación de servicios, bajas en el rendimiento y en general, que los usuarios no se vean afectados cuando accedan a los servicios.

3.1.3 Aseguramiento de software instalado

Con el crecimiento y la expansión del uso de las tecnologías de la información, se ha hecho necesario desarrollar cada vez más software, tanto privativo como libre. Al mismo tiempo, mediante la explotación de errores sutiles de programación o dependiendo del contexto, los hackers han sido capaces de manipular los sistemas para que operen como ellos deseen.

Entre las vulnerabilidades de software más reconocidas, se encuentra el desbordamiento (overflow) de búfer, que es un error de programación común que puede llevar implicaciones complejas. Los desarrolladores a menudo asignan una determinada cantidad de espacio de memoria temporal, llamado buffer, para almacenar una pieza particular de información. Si el código no es cuidadoso con la comprobación del tamaño de los datos respecto al tamaño del contenedor que los almacena, la memoria junto al espacio asignado está en riesgo de sufrir una sobrescritura (overwritte). Por tanto, el software puede vulnerarse si introducen cuidadosamente estructuras de datos que pueden bloquear el programa, o en el

peor de los casos, ejecutar códigos arbitrarios, llevando al colapso del sistema al ejecutarse este software.

Así mismo, la gran cantidad de exploits de desbordamiento de búfer en los que se han presentado en el pasado, hacen que los programadores tengan mucho más en cuenta estos aspectos a la hora de probar el software. Aunque los problemas de desbordamiento de búfer se siguen produciendo, a menudo son rápidamente descubiertos y corregidos, especialmente en las aplicaciones de código abierto. También, los nuevos sistemas de programación tales como Java y .NET, incluyen mecanismos que comprueban automáticamente los tamaños de los datos y evitando los desbordamientos de búfer.

En general, un software no se puede asegurar en su totalidad, ya que éste se crea para su total funcionalidad y sin muchas configuraciones de seguridad por defecto, luego, es una labor administrativa asegurar el software lo más posible, pero sin vulnerar la funcionalidad necesaria para que los usuarios puedan acceder a los contenidos. Los detalles técnicos del proceso de configuración y aseguramiento de los equipos de servidores no se muestran detalladamente, ya que no son documentos de acceso público.

3.1.3.1 Configuración y aseguramiento del servidor web Apache

Como ya se mostró en 2.3.1, el servidor web apache está constituido de forma modular, su estructura está conformada por un núcleo que llama a diferentes módulos que le dan funcionalidad. Luego, la labor administrativa se centra en configurar adecuadamente los módulos, asegurando la prestación adecuada del servicio sin que la seguridad se vea afectada.

El primer paso para el aseguramiento del servidor apache es definir el dominio web, los tiempos de respuesta, tiempos de sesión, los puertos disponibles y definir la ruta al directorio raíz donde se alojan los sitios web. El dominio web es el

nombre de dominio que es identificable en internet, en este caso, los servidores cuentan con un dominio que finaliza con la extensión *.uis.edu.co*, que es el dominio público de internet con el que cuenta la Universidad Industrial de Santander, por su parte, los tiempos de respuesta y de sesión son configurados en segundos, y se ajustan según las necesidades y requerimientos del servicio web que se desea prestar.

Con estos parámetros definidos, los accesos quedan ajustados a las necesidades básicas, pero aún la seguridad es mínima, ya que cualquier usuario podría recorrer todos los directorios y todos los documentos web que se encuentren alojados en el directorio raíz del servidor apache, además los paquetes de datos no son cifrados, por lo que la navegación en este punto aún no es muy segura.

Con el análisis de riesgo anterior, el siguiente paso es observar todo lo referente a permisos de los directorios disponibles en el directorio raíz web, si bien los sitios web se deben copiar con permisos de ejecución, se puede restringir los permisos a los usuarios y grupos adecuados, es decir, no dar todos los privilegios a todos los usuarios y grupos. De igual forma, en el archivo de configuración principal, se deben configurar los sitios que van a estar disponibles para los usuarios normales que acceden al servicio vía web, teniendo acceso únicamente a los sitios que se encuentran explícitamente en dicho archivo; cada vez que el servidor recibe una solicitud, identifica la ruta ingresada en el navegador y la asocia con el sitio web que tiene asignada dicha ruta en el archivo de configuración principal. Teniendo el servidor identificado el documento solicitado, este devuelve la respuesta al cliente.

La respuesta al cliente, al igual que las solicitudes, en este punto no tienen cifrado en sus datos, es decir, datos tales como contraseñas y nombres de usuario, viajan por la red sólo con la seguridad brindada por los protocolos de comunicación de red, sin ningún tipo de encriptación. Es así como se ha optado por añadir la característica de navegación segura HTTPS (Http seguro); para este propósito,

existe el paquete de software libre llamado OpenSSL, que incluye librerías de encriptación tanto del protocolo SSL (Secure Socktet Layer) como del protocolo TLS (Transport Layer Security), que añaden seguridad a los paquetes de datos que viajan por la red. Este paquete software opera en la capa de transporte del modelo OSI (Open System Interconection). Esta es la principal diferencia entre Http y Https, el primero opera en la capa de presentación del modelo OSI mientras que el segundo opera en capas más bajas gracias al uso de SSL/TLS, cifrando el mensaje enviado por una solicitud HTTP previa a la transmisión y descifrándolo una vez recibido.

La navegación segura de SSL, está basada en el establecimiento de un canal de conexión seguro, por medio de un proceso de autenticación, con el que posteriormente el cliente y el servidor están plenamente identificados. Este proceso de autenticación cliente-servidor por medio de SSL se basa en el uso de certificados digitales que contiene una clave (pública o privada) para el cifrado de los datos además de otra información, como nombre del sitios, la organización, país, ciudad, entre otros.

Dichos certificados pueden ser expedidos por una Autoridad Certificadora (CA) que de fe, por medio de una firma digital, que el servicio al cual está accediendo el cliente es de un servidor de confianza; de igual forma, el certificado puede ser creado por personal administrativo del servidor y auto-firmado, con lo cual el cliente debe está plenamente consciente del sitio al cual quiere acceder antes de su ingreso para que esté seguro que está accediendo a un servicio confiable. Los certificados expedidos por Autoridades Certificadoras tienen valor económico y regularmente tiene vigencia de un año, por tanto, dependiendo del tipo de servicio web que se desee brindar, se acude a estas autoridades certificadoras o se crea un certificado libre, por administrativos locales, el cual no genera ningún monto económico.

Para el actual proyecto, se ha implementado un certificado autofirmado para el servicio HTTPS, en el cual los servidores, al pertenecer al dominio educativo uis.edu.co y al tener uso netamente académico y no comercial, pueden prestar los servicios web con seguridad y sin mayores contratiempos, además al contar con el protocolo TLS, aporta un mayor grado de seguridad a las conexiones y a los datos que tanto el cliente como el servidor, intercambien en las interacciones que se tengan cotidianamente.

Para tener una visión más clara del proceso de autenticación cliente-servidor, se muestra a continuación un esquema que describe el proceso ya mencionado.

Figura 11 Proceso de autenticación para conexión segura SSL. Fuente http://publib.boulder.ibm.com/infocenter/tivihelp/v5r1/

La gráfica describe siete pasos para el proceso de autenticación de identificación cliente-servidor:

1- El cliente establece contacto con el servidor, este paso se describe como mensaje de saludo o “clientHello”.
2- El servidor responde enviando su certificado que contiene los parámetros mencionados anteriormente y con el cual se hace identificable al cliente.
3- El cliente verifica y valida el certificado que recibe, comparando con el almacén de claves. Si es la primera vez que accede al servidor web, el

cliente una vez validado, guarda los datos del certificado para posteriores ingresos.

4- El cliente para probar la identidad del servidor, envía una solicitud de identificación para el establecimiento de la conexión segura.
5- El servidor utiliza su clave privada para generar un mensaje de respuesta.
6- El servidor envía el mensaje cifrado al cliente.
7- El cliente descifra el mensaje utilizando la clave pública incorporada en el certificado firmado que recibe, con lo cual verifica la identidad del propietario del certificado y del servidor al cual está accediendo.

Después de este proceso, se establece un canal de conexión segura en el cual todos los datos que viaja por la red entre el cliente y el servidor son encriptados. El protocolo SSL y TLS son ampliamente utilizados para las conexiones cliente-servidor de los protocolos HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol) y NNTP (Network News Transport Protocol).

En el presente proyecto, el uso de SSL/TLS se ha implementado para el servicio web Apache, el cual, al incluir los módulos de SSL/TLS, puede operar con dos Host Virtuales, uno para la resolución de servicios HTTP y otro para las HTTPs, esto es debido a la operación en diferentes capas del modelo OSI de ambos. En la siguiente figura se muestra un esquema funcional que describe el comportamiento del servidor web en relación con las solicitudes y respuestas al cliente.

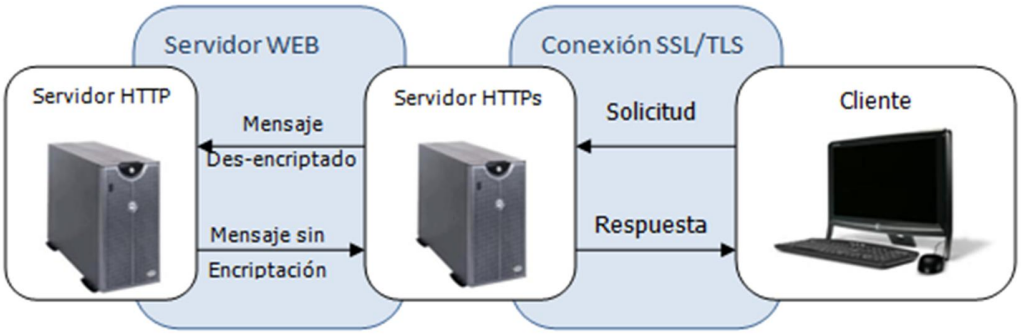

Figura 12 Esquema de funcionamiento de Servidor web con HTTPS

Los módulos de HTTPs, al operar en la capa de transporte, son los encargados de la recepción de las solicitudes y envío de respuestas al cliente (posteriores al proceso de autenticación descrito en la figura 11), mientras que HTTP opera en la capa de aplicación y es el que procesa finalmente el mensaje del cliente. Es de resaltar que en la parte del servidor todas las solicitudes recibidas son procesadas por los módulos del servidor web que operan bajo SSL, que decodifican la información cifrada y la entregan en un formato en el cual el servidor pueda procesar la información de la solicitud y de esta manera poder generar la respuesta. De igual forma, la respuesta del servidor HTTP, es enviada a los módulos SSL que realizan el proceso criptográfico y envían la respuesta HTTPS al cliente, con lo cual, el tránsito en la red de los datos en la comunicación se realiza de manera cifrada.

De este modo se consigue que la información ingresada por el usuario, como contraseñas y demás información sensible, sea imposible de utilizarse por un atacante que consiga interceptar la transferencia en la conexión, ya que lo único que podría obtener son datos cifrados, que resultarían casi imposibles de descifrar.

Con las configuraciones mencionadas y mirando periódicamente las actualizaciones de seguridad del equipo de desarrollo del proyecto apache e instalando las que se considere más prioritarias, puede decirse que la probabilidad de vulneración del sistema por parte del servidor web es baja, a su vez, la posibilidad de infiltrado en los datos de los usuario por interceptación de comunicación son igualmente muy bajos, aunque como ya se mencionó anteriormente y es de amplio conocimiento público, un sistema visible en internet nunca es completamente seguro.

3.1.3.2 Aseguramiento del gestor de bases de datos MySQL

Posterior a la instalación del gestor de bases de datos MySQL, la primera acción de seguridad que se debe realizar es la verificación de la funcionalidad del mismo, revisar la base de datos principal que se instala por defecto y las librerías incluidas, con lo cual se puede dar el aval para la creación de las diferentes bases de datos de los servicios del sistema que lo requieran.

Así mismo, se ha creado diferentes usuarios para la administración de las distintas bases de datos creadas, de modo tal, que la base de datos que pertenezca a un servicio específico sólo pueda ser accedida por un usuario de MySQL concreto. En este caso, por ejemplo, el usuario asignado para la administración de las bases de datos de Meiweb, no interfiere ni pueda ver o modificar las bases de datos de otros servicios, por ejemplo las bases de datos usadas por Moodle o los otros servicios incluidos y que dispongan de base de datos. Esto facilita, y organiza en cierto modo la labor administrativa, ya que no todos los usuarios de MySql tienen acceso a todas las bases de datos y se protege el ingreso exclusivamente de usuario root de MySQL a los administradores del sistema general.

Para controlar los permisos asignados a los usuarios de MySQL y garantizar que se han otorgado de manera adecuada para sus respectivas bases de datos, el gestor de bases de datos dispone de las sentencias GRANT y REVOKE; el primero para asignar permisos y el segundo para quitarlos. Esto se hace accediendo desde la cuenta principal de administración root de MySQL. De igual manera, para visualizar los permisos de cada usuario luego de las asignaciones, se utiliza la sentencia SHOW GRANTS que muestra cada permiso concedido sobre las bases de datos. Es de aclarar, que para cada usuario MySQL sólo es visible las bases de datos que se le han dado, lo cual ayuda a mantener el desarrollo independiente de cada servicio, y se evita interferencias entre estos. Únicamente el usuario administrador tiene control de todo el sistema de base de datos, aunque teniendo claro que la tarea administrativa se encuentra distribuida.

Otro aspecto de seguridad importante que se ha tenido en cuenta es la seguridad a nivel de usuario común, el cual accede a las bases de datos a través de los servicios web. El nivel más importante es la protección de los datos suministrados por el usuario por la web, estos viajan cifrados y son resueltos por el servidor Apache, PHP y/o Tomcat (dependiendo del sitio web) y redirigidos a la base de datos respectivas por medio de consultas SQL.

Como la administración de MySQL se puede realizar remotamente, existen variadas forma de realizarla, las más relevantes son las de vía grafica y las que utilizan líneas de comandos y se ejecuta desde una terminal. En cuanto a las herramientas gráficas, PhpMyAdmin es un entorno web de amplio dominio público, que presenta una interfaz web muy amigable, pero no es muy recomendable para administración segura, debido a las implicaciones que lleva tener dependencias de seguridad de lenguajes como PHP, sus actualizaciones de seguridad y lo que implica trabajar con versiones desactualizadas, los exploits que puedan tener el código de la versión del paquete, entre otros.

Por tal motivo es importante el uso de los medios no gráficos para la administración, por este medio se puede establecer mayores niveles de seguridad en los datos que viajan por Internet cuando se realiza la conexión remota. Para este fin se cuenta en los servidores Delfin y Sistemas con el protocolo de comunicación SSH (Secure Shell) el cual trabaja con técnicas de cifrado de los datos, y previene que los datos que viajan por la red sean vistos en su estado natural por terceros que puedan interceptar la comunicación. Para visualizar de una forma sencilla las diferentes formas de acceso al Gestor de bases de datos MySQL en los servidores Sistemas y Delfín, se muestra a continuación un esquema básico que representa dicho proceso:

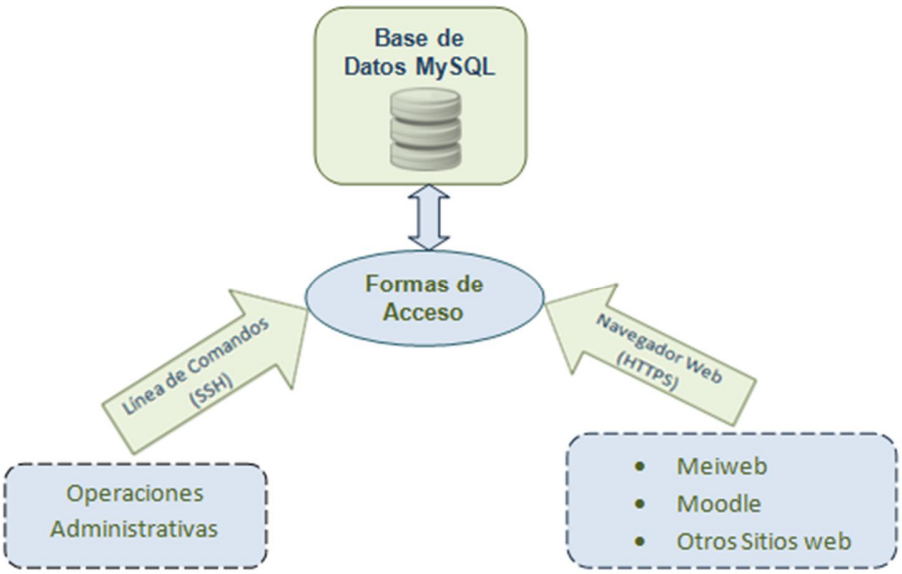

Figura 13 Esquema de Acceso al Gestor de Bases de Datos MySQL

Cabe destacar que la labor administrativa, dependiendo de la estructura de la codificación sitio web alojado, no depende exclusivamente del acceso administrativo por línea de comandos, ya que la mayoría de sitios web, como Meiweb y Moodle, cuentan con un entorno de administración de las tareas básicas del sitio, tales como, creación y modificación de usuarios, inserción, modificación y eliminación de datos de usuario, entre otras, que se pueden realizar por dicha interfaz propia y por navegación HTTPS. Luego, el acceso administrativo por línea de comandos puede limitar a tareas más complejas como modificación de tablas, cambios de llaves primarias y cambios en la estructura general de la base de datos.

3.1.3.3 Aseguramiento del software del lenguaje PHP

Tanto en el servidor sistemas como el delfín, se han configurado el paquete software del lenguaje PHP5 para que opere como módulo extra del servidor Apache. Es decir, los contenidos de los sitios web realizados en PHP, son procesados por el servidor apache y todo aquel contenido que no sea HTML puro y que sea asociado a la extensión *".php"* es procesado y ejecutado por los

módulos PHP5. Esta forma de trabajo modular es muy eficiente para el procesamiento de las solicitudes y las respuestas en la interacción cliente-servidor, ya que todos los datos pueden ser direccionados por un mismo puerto de comunicación y no por puertos diferentes

Ser un módulo funcional de Apache y no un programa que desempeñe sus labores independientemente, lleva consigo mismo ciertas implicaciones de seguridad, la principal es que PHP pasa a ser controlado por el usuario de Apache (usuario del sistema que ejecuta el servidor Apache) y por tanto hereda sus permisos, luego, si dicho usuario tiene más permisos de los necesarios para su normal funcionamiento, podría generar una condición de riesgo alta y a comprometer el sistema mismo. Para evitar esto, se han tomado una serie de medidas preventivas, de las cuales se hará mención en la sección 3.2 (Gestión de Usuarios y Grupos).

Entre los factores a tener en cuenta, se encuentra el hecho de que el PHP es un lenguaje que permite al usuario interactuar con bases de datos alojadas en el servidor y muchas veces los desarrolladores desconocen muchas de las características de seguridad básicas, con las cuales los usuarios maliciosos podrían hacer ataques y vulnerar la base de datos. Para esto, se debe tener en cuenta la restricción del uso de caracteres tales como “%”, “=”, “ ’ ”, entre otros, para los campos de tipo numérico (integer, double, float) y alfabético (carácter).

Así mismo, el bloqueo a los registros globales, ya que esta función puede generar ambigüedades y otro tipo de problemas que podrían generar huecos de seguridad, aún inadvertidamente. Su uso está totalmente desaconsejado desde las versiones más recientes del PHP (Versión 5.3.0 en adelante), y por tanto bloqueado en el sistema. Cabe mencionar que los servidores trabajan con varias versiones de PHP simultáneamente, con lo cual se ha tenido similar tratamiento en materia de

seguridad para las diferentes versiones manejadas, ya que la configuración de seguridad no varía mucho de una versión a la otra.

Dentro de la estructura de seguridad se ha considerado el aspecto de seguridad de los tiempos de sesión para las solicitudes de los usuarios. PHP ofrece dentro de su estructura de configuración una serie de sentencias con las cuales se puede restringir aspectos tales como, tiempo de vida de una sesión tras un periodo de inactividad, tiempo de expiración de una solicitud, período de vida para las cookies de navegación, entre otros, que permiten que tanto el usuario como el servidor mantenga una conexión segura, evitando incidentes involuntarios a nivel de usuario, tales como, sesiones abiertas en computadores públicos y demás.

En cuanto al reporte de errores, PHP cuenta con la opción de activar o desactivar las directivas que se utilizan para tal fin. Evidentemente este tipo de información debe ser transparente para el usuario y sólo es pertinente para los desarrolladores de las aplicaciones web y durante la etapa de desarrollo, por tal razón, estas directivas se han desactivado para evitar inconvenientes que podrían generar ataques y fallos en la seguridad.

En cuanto a seguridad, constantemente se lanzan diferentes actualizaciones de seguridad por parte de la comunidad de desarrolladores, de igual manera, se publican diferentes huecos de seguridad presentes y parches para su respectiva corrección, por tal motivo, dentro de las políticas de seguridad, se contempla la revisión periódica de dichas novedades con lo cual se puede mantener el sistema y los servicios seguros y su probabilidad de vulneración sea menor.

3.1.3.4 Seguridad del Agente de Correo

El agente de envío de correo configurado en los servidores, se encuentra compuesto de diferentes paquetes software que hacen posible mantener un esquema seguro y funcional para el envío de correos, contando con una

infraestructura robusta y de fácil manejo y monitoreo. Los paquetes software instalados cumple diferentes tareas para la gestión de correos.

El paquete Postfix tiene bajo su función el soporte de envío de correos de los usuario de las aplicaciones web y correos de usuario locales del sistema, ya que su rol es el de servir como agente de transferencia de correos (MTA) anfitrión. Para que la labor de dicho software se pueda mantener en condiciones seguras y los datos enviados por los usuarios mantengan su integridad y no sean fáciles de interceptar, su configuración cuenta con características de navegación segura al habilitar el protocolo TLS para la asistencia del envío SMTP, de igual manera dentro de sus opciones configurables, se encuentra la de deshabilitar TELNET, ya que sus características de seguridad no son muy favorables.

Para uso interno del agente de correo, se cuenta con el paquete SquirrelMail, que es una aplicación web escrita en PHP con la cual el personal administrativo puede gestionar diferentes aspectos funcionales para el envío de correos. Su funcionamiento óptimo se logra con el apoyo de los paquetes CyrusIMAP, que es un paquete software que da acceso a los correos almacenados en el servidor; para la gestión de listas de correos se cuenta con el software GNU MAILMAN y el envío de correo utiliza el Postfix. La seguridad de estos en su conjunto depende de la configuración del protocolo de comunicación utilizado por Postfix, anteriormente descrita, y la configuración de navegación del servidor Apache y de PHP también ya descritos en secciones anteriores.

Además de SquirrelMail, los sitios web alojados en los servidores que cuentan con la opción de envío de correos también requieren asistencia del MTA para el correcto direccionamiento del correo saliente, evitándole contrariedades a los usuarios de los servicios, por ejemplo, las plataformas MeiWeb y Moodle cuenta con estas opciones de envío de correos, luego es importante que sus datos viajen

por la red forma segura y que los protocolos de comunicación con TLS, HTTPS y SMTP se configuren para que su función sea correcta.

3.1.3.5 Aseguramiento del software del Alta Disponibilidad

El clúster de alta disponibilidad montado entre los dos equipos de servidores, se encuentra compuesto por un conjunto de paquetes software que en su configuración cumplen labores específicas, pero su conjunto operante componen el servicio funcional de alta disponibilidad. La función de cada software se describe en la sección 2.7.2.

Para la tarea de aseguramiento del clúster, se ha tenido en cuenta, en primer lugar el tipo infraestructura montado en los equipos servidores. Las diferentes formas de montaje del clúster de alta disponibilidad, se encuentran detallados en la sección 2.7.1; de todas las que se encuentran allí descritas, se ha elegido para el clúster de los equipos Sistemas y Delfín la infraestructura Activo/Pasivo, cuyo esquema se encuentra graficado en la figura 4.

Se ha elegido dicho esquema, por diversos motivos, entre los más importantes que se han tenido en cuenta es que en primer lugar se cuenta con dos nodos (equipos) para la creación del clúster, en segundo término, los otros tipos de infraestructura son más eficientes cuando se cuenta con una mayor cantidad de nodos, y el punto de consideración final para optar por dicha infraestructura, es por la administración misma de los servicios del clúster, ya que la integridad de los datos y los servicios compartidos son mucho más fáciles de asegurar con este tipo de infraestructura, pues los usuarios sólo acceden a los servicios en un nodo a la vez, ya que al tener un nodo activo y el otro pasivo, todos los servicios y recursos que forman parte del clúster de alta disponibilidad van a estar montados únicamente en el nodo activo, mientras el pasivo va a tener estos recursos en un estado de stand-by, cumpliendo con una labor de apoyo en caso de que se

presente fallos en el nodo que se encontraba inicialmente activo y tomando su rol posteriormente y montado los recursos y quedando este ahora como nodo activo.

La definición de los roles de activo y pasivo se da por reconocimiento en la red, es decir, los nodos están en constante comunicación por red para reconocer sus estatus permanentemente, para que así, en dado caso, la comunicación se vea interrumpida por cualquiera que sea el factor, el pasivo toma el rol de Activo y el servicio a los usuarios no se vea afectado por dicho asunto. Es ahí, en el modo de operación, donde se tiene en cuenta el primer y más relevante aspecto de seguridad, ya que es en la comunicación misma donde se puede ver vulnerado el sistema. Entonces, para disminuir la probabilidad de éxito de ataques por red a través del clúster, se ha creado una red local, con direcciones IP privadas, que son direcciones que difieren a las que normalmente se usan para acceder a los servicios vía internet.

Con la configuración de la red privada y añadiendo un cortafuegos (firewall), se puede mejorar sustancialmente la seguridad, no solo del clúster, sino del equipo en general. Así mismo, para la administración del clúster se ha creado usuarios del sistema, diferentes al usuario administrador principal root, para la administración del clúster dando otra característica de seguridad importante, ya que el control y la administración del clúster de alta disponibilidad no se da única al usuario root, sino que esta labor se encuentra delegada a otro usuario del sistema. Estos usuarios tienen restringidas otras tareas que no son propias de ello, con lo cual la seguridad del sistema se puede mantener.

De igual forma, los directorios del sistema y el disco lógico compartido en el clúster tienen acceso restringido únicamente para los usuarios y el grupo asignados para las labores de administración del clúster; luego, sólo estos y el usuario root del sistema tienen acceso a los directorios del sistema que conforma el clúster de alta disponibilidad. En la sección 3.2 (Gestión de Usuarios y Grupos) se menciona de

forma más concreta del proceso de asignación de permisos sobre ficheros y directorios y tipos de usuarios del sistema.

Con lo anteriormente descrito, se puede garantizar el servicio de alta disponibilidad para su uso por parte de los usuarios, sin sacrificar la seguridad del sistema, ya que con dichas configuraciones, todas las operaciones de alta disponibilidad se realizan por red local y son transparentes para los usuarios normales que ingresan por el dominio y la dirección IP pública.

3.1.4 Seguridad del acceso por red

Los equipos servidores al encontrarse ubicados en un lugar con limitación de acceso físico, casi la totalidad de los accesos al sistema de cada máquina se da por red. De igual manera, todos los usuarios acceden por navegador web a los servicios que allí se prestan, por lo que es muy importante que los equipos cuenten con protección de cortafuegos para limitar el acceso por puertos no deseados, así como acceso únicamente por protocolos de comunicación autorizados, entre otras características definibles según sea la herramienta a utilizar como Firewall.

El sistema operativo GNU/Linux cuenta en su núcleo por defecto, con una opción de cortafuegos muy eficaz y de fácil manejo llamado Iptables, con el cual se puede gestionar el tráfico de red de entrada y salida del sistema. Esta herramienta cuenta con un Framework que permite administrar los paquetes de datos que transitan desde y hacia el equipo, por medio de reglas definibles únicamente por el usuario administrador del sistema.

Por medio de estas reglas, el sistema define si el paquete de datos cumple o no con las características de seguridad dadas por estas, tales como el tipo de protocolo, puerto de red, entre otros, que hacen que en el sistema sólo ingrese información por red, según los parámetros definidos en cada regla.

Iptables es un paquete de software libre con licencia GPL, es sencillo de administrar y la creación de reglas cumple óptimamente con su labor, y al ser una aplicación propia del núcleo Linux, que éste trae por default, tiene un nivel de seguridad muy alto, que se puede mantener según las actualización en las versiones y paquetes de seguridad liberados por los desarrolladores.

3.2 GESTIÓN DE USUARIOS Y GRUPOS

La creación y manejo usuarios del sistema, conforman una parte muy relevante de la función administrativa, ya que la correcta o la incorrecta creación y uso de los mismos, puede generar un cambio notorio en los aspectos funcionales y de seguridad del sistema en general. Para evitar esto, el conocimiento básico del manejo de usuarios en sistemas Linux y el planteamiento o seguimiento de un modelo de organización de usuarios y grupos hace posible mantener el sistema en condiciones buenas de seguridad y la administración del mismo se puede realizar de manera controlada.

Es de aclarar que dentro de la gestión de usuarios en sistemas operativos Linux, éste le define un identificador (UID) a cada usuario creado y sus datos son almacenados en los ficheros *passwd* y *shadow*, esta información es de acceso restringido y sólo modificable por el usuario root del sistema. Todo usuario del sistema está asociado a uno o más grupos según sea su Rol en el sistema.

Un grupo es un esquema lógico, creado para reunir varias cuentas de usuario que tiene un propósito común, compartiendo los mismos permisos de acceso a recursos especificados para el grupo en el sistema. Todo grupo tiene un nombre y un identificador de grupo (GID) únicos y sus datos son almacenados en el fichero *group*, que al igual a los ficheros que contienen los datos de usuario, su manipulación se restringe al usuario administrador del sistema.

3.2.1 Control de acceso basado en roles

Para una correcta gestión de usuarios, en términos administrativos, se ha optado por seguir un modelo de gestión de acceso al sistema basado en Roles, es decir, según sea el papel que desempeñe cierto usuario, éste va a poder acceder y manipular recursos.

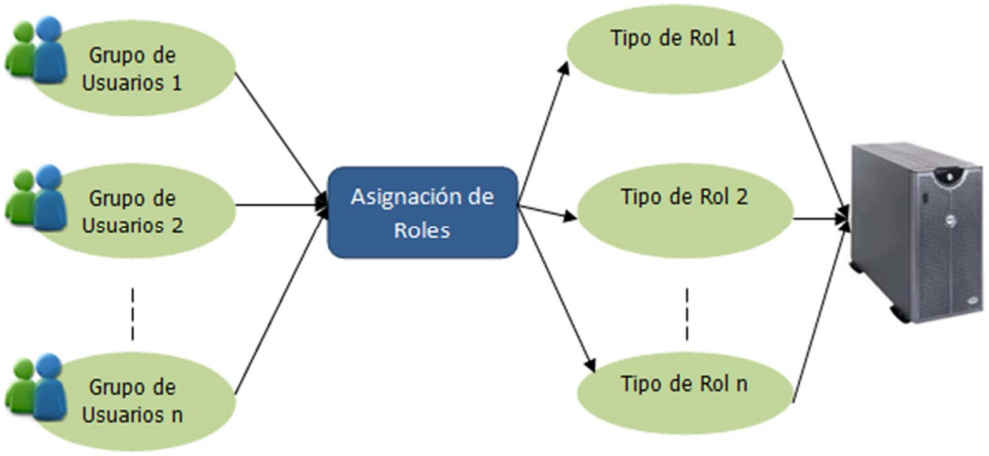

Figura 14 Modelo de control de acceso basado en Roles

El propósito fundamental que se desea lograr implementando este modelo, visible de manera general en la figura anterior, es tener la capacidad de delegar funciones administrativas, pero conservando los aspectos básicos de seguridad, de esta manera, no todo el peso administrativo recae sobre el usuario administrador principal root, sino que, según sea la tarea o rol administrativo, se crean el usuario y se le conceden ciertos permisos para que cumpla sus funciones.

Para la manipulación de directorios y ficheros, el modelo se sigue de la misma manera. Según sea el Rol del usuario en el sistema, se le otorgan permisos, ya sean de lectura, escritura y/o ejecución. Con esto, se puede proteger sustancialmente el sistema en general, ya que, únicamente usuarios administradores del sistema puede entrar a configurar ficheros de configuración del sistema, iniciar servicios, entre otras labores, que no podría realizar un usuario normal.

El S.O Debian GNU/Linux trae una estructura de seguridad muy importante por defecto, con lo cual la gestión de usuarios y grupos, así como, el manejo de los roles y los permisos sobre directorios y ficheros, se puede realizar de manera sencilla, llegándose a dejar implantado en el sistema una estructura administrativa consistente y altamente segura.

Este método de gestión es muy efectivo para mantener la estructura de seguridad del sistema, ya que no todos los usuarios van a tener acceso a todas las tareas, ni todos los usuarios van a poder acceder al sistema de la misma manera; ya que por seguridad, algunos de los usuarios que tienen misiones críticas no puede acceder directamente al sistema por acceso remoto.

Las formas de acceso al sistema y demás tipos de tareas, depende de los tipos de usuario que se consideran dentro de la gestión administrativa del sistema. Estos se describen a continuación.

3.2.2 Tipos de roles de usuarios

Para la creación de usuarios en el sistema, se ha considerado diversos aspectos fundamentales de seguridad, en especial aquellos que tienen relación con el acceso al sistema, las tareas administrativas y los servicios. Por tanto, cada usuario creado se debe ajustar a ciertas reglas y a cierto perfil, que se asignan según sea el propósito de su creación. Todos los usuarios, que no son creados por defecto en el sistema, deben crearse por el personal administrativo, considerando que dicha tarea se debe ajustar a los roles diseñados para el sistema. Estos roles se describen a continuación.

3.2.2.1 Rol de Usuario Administrador

El usuario administrador o usuario root, es el usuario que posee todos los permisos para todos los archivos y programas. Este usuario puede realizar diversas tareas que otros tipos de usuarios no pueden efectuar, tales como

cambiar el propietario de archivos y directorios, gestión de conexión de puertos en el sistema, entre otras la labores de gestión exclusiva.

Para otras tareas, que no son considerablemente críticas para la operación del sistema pero que son importantes para la prestación de servicios, se crean otros tipos de usuarios, manteniendo de esta manera el esquema de seguridad del sistema y éste sea menos propenso a sufrir vulneraciones; ya que dado al nivel de privilegios del usuario root, no es conveniente que todos los programas sean ejecutados o asociados directamente por él.

Entonces, basándose en criterios de seguridad y de funcionalidad, se han planteado otros tipos de usuarios diferentes al Administrador, según sea el tipo de tarea asignable y la conveniencia que conlleva su ejecución por parte de un usuario de carácter no-root. Estos roles de usuarios no administradores, se describirán a continuación, mostrando el papel desempeñado por estos dentro del sistema.

3.2.2.2 Rol de Usuario de Acceso

Son usuarios creados con el propósito exclusivo de acceder al sistema remotamente y el rango de tareas posibles para éstos es muy limitado, ya que no poseen permisos para gestión de servicios y sus tareas de escritura y ejecución se limitan a su propio directorio Home (/home/usuario) y a los archivos a los cuales el usuario administrador le asigne permisos fuera del directorio home. El propósito de crear cuentas exclusivas para acceso remoto, se debe netamente a la conservación de parámetros de seguridad, ya que, al restringir el acceso remoto únicamente para usuarios determinados, disminuye la probabilidad de éxito de los ataques por red.

Al tener la función de acceder remotamente, estos usuarios poseen características muy importantes de seguridad, en cuanto a criterios de creación y extensión de los

nombres y contraseñas de acceso; dado al carácter de esta información, su uso es netamente privado.

3.2.2.3 Rol de Usuario de Servicios

Algunos software, pueden configurarse de manera que varias o todas sus funciones estén disponibles para ejecución por parte de otros usuarios, como lo es el servicio de apache, que se ejecuta como demonio desde el kernel, al iniciar el sistema, pero las tareas y directorios pertenecen al usuario del servidor web.

Ante esto, se ha creado el rol de usuarios de servicios, cuya la labor es ejecutar aplicaciones, teniendo bajo su propiedad directorios específicos del servicio que se le ha asignado. Algunos de estos usuarios, según sea la naturaleza de su labor o del servicio a ejecutar, tienen características particulares y son personalizados para tal fin; entonces, dependiendo de cual su tarea, el usuario puede configurarse para contar con un bash específico para su trabajo, o carecer de éste si no es necesario que tenga login o contraseña en el sistema.

3.2.2.4 Rol de Usuario Jaula

Los servidores, al ser equipos orientados a labores académicas, sirven de apoyo a estudiantes durante su proceso desarrollo e investigación, sobre todo de servicios orientados a la web. Para lograr que estos estudiantes puedan acceder al sistema para hacer pruebas de sus proyectos, sin que se comprometa el esquema de seguridad y la integridad del sistema, éstos usuarios deben tener uso limitado de los recursos, pero teniendo en cuenta que estas limitaciones no afecte la funcionalidad de sus trabajos.

Por este motivo, a este tipo de usuarios se les asigna un ambiente limitado dentro del sistema, en el que pueden trabajar en sus tareas específicas, sin que ellos puedan intervenir en los demás aspectos del sistema. La acción a tomar para tal fin, es la creación de usuarios en “jaulas” chroot. En el entorno chroot, se crea

para el usuario un directorio raíz simulado, en el cual puede ejecutar sus diferentes aplicaciones y librerías, sin que sus acciones afecten al sistema completo; además, estos usuarios no podrán manipular archivos ni directorios fuera de su directorio raíz, teniendo un alto grado de seguridad, ya que el usuario no podrá realizar procesos de escalado hacia otros contenidos ni usuarios.

Se espera que a futuro y según sean las tareas que se deseen realizar sobre el sistema, se puede llegar a crear nuevos perfiles de acceso, pero considerando siempre los aspectos fundamentales de seguridad y la verdadera necesidad de la creación del nuevo rol y lo que dicha acción implica. Todo rol y todo usuario, antes de ser creado debe tener una evaluación por escenarios, para que de esta forma aprobar o descartar tal acción.

3.3 GESTIÓN DE RECURSOS

Los recursos instalados en los equipos, en especial los servidores web Apache y los que se relacionan con éstos, requieren de tareas periódicas en las cuales se debe buscar que los usuarios gocen de un buen servicio con el menor número de percances posibles; para ello, se busca implementar mecanismos con los cuales se pueda volver a un estado anterior en caso de que se presente algún comportamiento no esperado en los servicios prestados o se den fallos de carácter humano.

Al mismo tiempo, los dos equipos servidores conforman un clúster de alta disponibilidad en el cual se incorporan los servicios prestados y discos con datos compartidos que se montan según la infraestructura de clúster implementada. Por tal motivo, se debe mantener un constante monitoreo de dichos recursos, al mismos tiempo que se automatizan tareas básicas y de esta forma la función administrativa se realice de manera eficaz y a su vez, las tareas propias de la gestión sea de fácil manejo.

En los siguientes apartados se describirán los diferentes procedimientos con los cuales se busca que dichas proyecciones administrativas sean realizables. Para poder cumplir con dichas tareas, se ha planteado la gestión de recursos, lo cual representa las acciones permanentes de la función administrativa durante la mayor parte del tiempo en que se encuentre en producción los equipos servidores.

3.3.1 Copias de seguridad del sistema

El sistema operativo de los equipos es el software fundamental implantado, de su correcto desempeño, depende la funcionalidad de todos los servicios, por tanto, luego de su instalación, la configuración y los ajustes de seguridad del software para servicios, es importante tener imágenes de respaldo del sistema operativo, para que en determinado caso, se pueda regresar a estados anteriores del sistema.

Las fallas en el Sistema Operativo se pueden presentar por una gran diversidad de factores posibles, desde fallos en la instalación de actualizaciones, hasta ataques por la web. Además, considerando que los equipos están permanentemente conectados a Internet el riesgo de fallas provocadas es aún mayor. De igual manera, puede ocurrir daños, en el software de servicios, en los cuales, hasta una mala configuración podría estropear la operación del mismo.

Entonces, considerando los diferentes escenarios en los que el sistema podría caer en condición de error, se deben crear backups del sistema, en diferentes tiempos, en los cuales se respalde el sistema en diferentes etapas. Con esto se podría abordar el problema de manera oportuna y los servicios no sufrirían ninguna alteración.

Dado a que cada imagen puede llegar ocupar espacios de disco de tamaño considerable, no es adecuado contar con muchas imágenes del sistema, pues el espacio no es ilimitado y debe disponerse espacio suficiente para soportar

información de los servicios y de los usuarios y para servicios que se deseen ofrecer a futuro; por tanto, la elección del momento adecuado para realizar cada respaldo debe ser analizado cuidadosamente pero también en un momento oportuno.

La copia de seguridad que podría considerarse de mayor utilidad es la que se realiza después de que se han realizado las configuraciones básicas de seguridad del sistema y los servicios se han adecuado para que su funcionamiento sea el adecuado; esto se menciona como un momento crítico, ya que es en este instante cuando el sistema se considera apto para estar en producción y conectado en la web.

Al realizar el proceso de restauración del sistema, se debe tener en cuenta los procedimientos para la puesta en marcha de los servicios nuevamente; los aspectos tales como los datos de los usuarios de los servicios web y las bases de datos en general, deben quedar nuevamente en un estado funcional óptimo, para que de esta manera el usuario presente la menor cantidad de molestias posible que se puedan generar a causa de dicha acción.

3.3.2 Migración de servicios

Los nombres Sistemas y Delfín con los cuales se distinguen los servidores, provienen de equipos que ya se encontraban en producción anteriormente, trabajando con los dominios de internet sistemas.uis.edu.co y delfin.uis.edu.co respectivamente. Con la llegada de los nuevos equipos, los sitios web que se encuentran alojados en las máquinas antiguas deben trasladarse a las nuevas, teniendo en cuenta que dicho proceso debe ser lo más transparente posible para los usuarios normales, evitando molestias en la prestación del servicio; además de considerar todos los aspectos de seguridad posibles para que los datos transferidos de una máquina a la otra se mantengan correctos y completos.

Para el logro de tal propósito, se ha realizado un análisis de los requerimientos de versiones del software bajo el cual los servicios de los sitios web en producción pueden trabajar en óptimas condiciones, a su vez, se ejecutaron pruebas de funcionamiento bajo versiones más actuales. Esto se realiza debido a que en el software del lenguaje PHP específicamente, puede presentarse variaciones en las librerías de una versión a otra, con lo cual algunas variables y/o métodos del código de las páginas no sea compatibles con versiones más recientes, repercutiendo en la correcta operación de los servicios web.

Ante esto, se optó por trabajar para los sitios web migrados a las máquinas nuevas, con la versión correspondiente a la instalada en los equipos antiguos y con la cual los servicios no presentan ningún inconveniente; pero, para no limitar los equipos a versiones antiguas del PHP, se instaló también una versión reciente estable. De esta manera, se puede garantizar que a futuro, nuevos servicios web puedan ser alojados y su funcionamiento sea correcto en los equipos.

Para que operen simultáneamente dos versiones diferentes de PHP, se tuvo en cuenta la funcionalidad del servidor Apache. Para esto, se evaluaron las diferentes formas de funcionamiento del servidor web apache junto las dos versiones del lenguaje PHP, pero dado a que Apache trabaja de forma modular, sólo puede funcionar con una versión de PHP a la vez, es decir, se pueden tener varias versiones de PHP instaladas, pero si sólo hay un servidor Apache ejecutándose, éste sólo puede reconocer una versión de PHP a la vez.

Para lograr tal simultaneidad sin entrar en conflicto con el servidor web, se ha optado por la instalación de dos servidores Apache, cada uno teniendo asociada una versión del PHP, logrando que un servidor apache tenga asociada la versión antigua del lenguaje y el otro a su vez ejecute la versión reciente.

Ante la necesidad de instalar dos servidores web, para que puedan funcionar simultáneamente en el mismo dominio de internet, se han configurado para que transmitan y reciban datos por puertos de red diferente, de esta manera ambos pueden tener acceso sin limitantes de carácter técnico debido a conflictos de versiones. Cabe resaltar, que los dos servidores Apache instalados, son diferentes versiones, pero corresponden a lanzamientos recientes, ya que durante las pruebas realizadas, se verificó que éstos pueden funcionar con los módulos de PHP sin que la versión de este lenguaje sea un factor que afecte su funcionalidad.

En cuanto a los demás software implantados en los equipos, todos se han instalado en versiones recientes estables, sin que esto afecte en ningún aspecto la prestación de servicios de los sitios web migrados. Al completarse el proceso de migración, los equipos nuevos han entrado en operación, dando paso a sus configuraciones de seguridad y a todo lo que esto implica en la gestión administrativa.

3.3.3 Copias de seguridad de los servicios

Al igual que el sistema operativo, los servicios ofrecidos a los usuarios están sujetos a errores y fallos, los cuales en la mayoría de veces llegan a ser ocasionados, no por vulneraciones de seguridad, sino por error humano, en gran parte porque se deben a que brindan servicios académicos y los cambios en la información se realizan de manera permanente.

Son los cambios en los datos de los usuarios y en las bases de datos de los sitios web donde repercute la gran parte de los errores y fallos; a su vez, son estos contenidos importantes para que los sitios web ofrezcan un adecuado servicio, ya que los usuarios requieren que toda su información esté disponible e integra en cualquier instante en que desee ingresar a su cuenta en el sitio web que utilice. Entonces, analizando los escenarios en los cuales se llegan a presentar inconsistencias del carácter anteriormente nombrado, y que éstas no se puedan

solucionar totalmente por los administradores de los sitios, o la información no sea recuperable por esta vía, la solución se encuentra en la creación de un esquema de Backups periódicos.

Al realizarse copias de seguridad de los datos y de las bases de datos de los sitios, aunque no se elimine el problema, es una salida eficaz este asunto, ya que en caso de que se presenten tales situaciones se puede recurrir a algunas de las copias de seguridad y hacer su restauración, según sea la situación y según sea conveniente. En vista de la utilidad de los respaldos a la información de los sitios web, lo siguiente a tener en cuenta es la periodicidad y el tipo de backup que se realice.

Para esto, debe plantearse un esquema de backups, en el cual se optimice el proceso y se realicen los respaldos de la forma más conveniente para la administración de los servicios, ya que, si no se optimiza el proceso de creación de backups, se puede llegar a tener una desorganización en los directorios o discos en los cuales se almacenan, lo cual haría muy tediosa la tarea administrativa, que además podría repercutir en un uso inadecuado del espacio de disco. Para evitar los problemas mencionados, se pueden crear diversos tipos de backups. Existen diversos tipos y estilos de creación de copias de seguridad, para evaluar la mejor opción, se tuvo en cuenta el tipo de servicio que se presta, que es de tipo académico, además se pensó en la interacción de los discos que guardan los directorios de los backups en relación con el clúster de alta disponibilidad, entre otros aspectos que hicieron posible la creación de tal esquema funcional.

Los tipos de backup implementados en los equipos son los de carácter completo e incremental, ya que son de fácil administración y cumplen eficazmente la labor de respaldo. Los backups completos son los que generan copia de todos los archivos que se encuentran dentro del directorio a respaldar, es el más común y de uso más expandido. Los backups incrementales, sólo generan copia de

seguridad de aquellos archivos que hayan tenido modificaciones (posteriores a uno incremental de referencia) en el directorio a respaldar.

Conociendo como operan los dos tipos de backups, se procede a diseñar el esquema de creación periódica de los respaldos. Se ha optado por crear uno completo semanal y los días restantes se crearán incrementales, uno cada día; así mismos se ha tenido en cuenta que la realización de éstos se efectuará en horarios en los cuales no se afecte el servicio a los usuarios. En la siguiente gráfica se describe el esquema de copias de respaldo que se ha adecuado en los equipos.

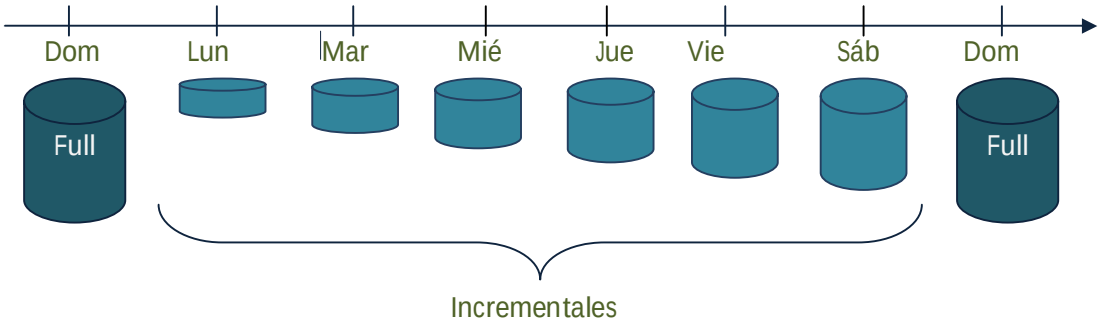

Figura 15 Esquema de respaldos periódicos locales

Con este esquema de creación de copias de respaldo, el espacio en disco y la organización de las copias se optimizan notoriamente al tener distinción por fechas; además las copias incrementales se sobrescriben de una semana a otra, evitando tener demasiadas copias incrementales, ya que cada fin de semana se realiza un nuevo backup completo, por lo que todas los cambios que se realizaron durante la semana quedan guardados en dicho archivo de respaldo.

Es decir, al implementarse el esquema de generación de copias de seguridad representado en la Figura 15 y luego de una serie de pruebas de funcionamiento realizadas en un entorno controlado de máquinas virtuales, se infiere que el esquema implementado funciona adecuadamente para el entorno de trabajo, ya

que, por una parte, se asegura la creación en una forma lineal de los completos, mientras los incrementales se generan por ciclos semanales sobrescribiéndose los de la semana anterior. De esta manera, los backups completos se almacenan y se mantienen como plan de contingencia en caso que se requiera restaurar una copia relativamente antigua, mientras que los incrementales se mantienen los actualizados de la semana, en caso que se requiera una copia generada durante la semana en curso y no recurrir únicamente al backup completo de la semana inmediatamente anterior. Con lo anterior, se garantiza que los datos respaldados se puedan restaurar si las circunstancias lo requieren, al mismo tiempo que se optimiza el espacio y se mantiene un control organizativo de los mismos.

La tarea de realización de backups se podría realizar todos los días de forma manual, pero esta es una tarea repetitiva, que se puede optimizar por procesos de automatización en el sistema. Esto es descrito con mayor detalle en la sección 3.4 (Automatización de Tareas Administrativas.)

3.3.4 Revisión de Logs del Sistema

Dentro de las tareas administrativas, una de las más importantes es la de mantenerse al tanto de los eventos ocurridos en el sistema. Para apoyo de esta labor, el sistema operativo guarda registros de las aplicaciones que se ejecutan; guardando datos detallados, tales como, el nombre de la aplicación, hora de ejecución, quién la ejecutó, porqué, etc. Este nivel de detalle es muy importante, en términos administrativos, porque estos archivos de logs, guardan toda la información suficiente para estar al día acerca de lo que acontecen en los equipos, con lo cual se facilita la toma de decisiones, y actuar de manera acertada al momento de presentarse un comportamiento no deseado en el sistema.

Revisar cada registro, uno por uno, sería una tarea administrativa poco eficiente, ya que tomaría demasiado tiempo la realización de dicha labor, ya que diariamente se genera una gran cantidad de registros en los ficheros de Logs.

Ante esto, se ha optado por la instalación de la herramienta Logwatch, con la cual se hace una recopilación de los eventos más importantes ocurridos en el sistema y se envían por medio de smtp al correo de los administradores.

Logwatch es una aplicación de software libre, con licencia x11 de libre distribución, y funciona recolectando información a través de los archivos de logs por un período de tiempo determinado y genera un reporte en las áreas que se le han especificado en sus ficheros de configuración y con el nivel de detalle que se desee. Es fácil de configurar y la tarea de generación de los reportes es automatizable.

3.4 AUTOMATIZACIÓN DE TAREAS ADMINISTRATIVAS

Dentro de las funciones de los administradores, existen diversas tareas cuyos procedimientos se pueden automatizar. Entre las tareas automatizables se encuentran las de generación de respaldos, generación de informes de logs del sistema y en general todos aquellos procesos administrativos del sistema que se realizan periódicamente. Además de procesos más complejos como lo son la creación de usuarios, que si bien no se hacen con periodicidad, también son automatizables.

Con la creación de tareas administrativas automatizadas, además de ganarse en eficiencia para la gestión de tareas cotidianas, se puede tener mayor seguridad de que aquel proceso se hará de manera correcta, ya que no está sujeto a fallas de digitación de comandos o fallas humanas, ya que el procedimiento se encuentra codificado en scripts de Shell, con órdenes interpretables por el sistema operativo.

Los scripts de Shell, son piezas de código, con el cual se especifican órdenes que se comunican con el núcleo del sistema; al momento de ejecutarse el script, éste es interpretado y el sistema realiza instrucciones allí dadas. Un script puede contener desde una sencilla orden hasta un conjunto estructurado y complejo de

variables y comandos que controlan aspectos críticos del sistema. Es por esto que se debe tener en cuenta los permisos y propietarios de dichos scripts, ya que al otorgar permisos inadecuadamente podría generar mayor probabilidad de riesgo de vulneración del sistema.

Ante esto, los scripts creados para tareas administrativas sólo tienen permisos específicos y son propiedad del usuario administrador, mejorando las características de seguridad del sistema, al mismo tiempo generando un ambiente administrativo optimizado, ya que ningún otro usuario podrá tener acceso alguno al código ni ejecutarlos. Por otra parte, los scripts creados para la realización de tareas periódicas, son incluidos en las tablas de ejecución de tareas programas del sistema, logrando que éstos sean ejecutados como demonios según sean los intervalos programados para cada uno. Los nombres de los scripts, su código y ubicación privados y referenciados en la documentación administrativa interna.

3.5 MANTENIMIENTO

Los equipos poseen en su mayoría software en su última versión estable, pero dado a que éstos son en su totalidad paquetes de software libre, están sujetos a muchas actualizaciones, incluyendo el sistema operativo Debian y su kernel Linux. Por tanto, es muy importante para que el equipo permanezca en buenas condiciones de seguridad y se brinde un buen servicio, realizar periódicamente las actualizaciones que se consideren críticas o de mayor prioridad.

Así mismo, se debe tener en cuenta el hardware y su funcionamiento adecuado, observando especialmente elementos críticos y propensos a mayor deterioro por el uso, tales como los discos duros (a nivel físico) y sus esquemas de particionado (a nivel lógico), ya que según sean las condiciones del entorno físico (temperatura, humedad, etc.), el desgaste provocado por el tiempo y el uso y la calidad misma del disco, el deterioro de éstos puede acentuarse en una mayor o menor medida.

Ante esto, se han creado una serie de funciones y procedimientos para la realización labores de mantenimiento, tanto preventivo como correctivo, por medio de análisis de escenarios, que puedan generar situaciones que repercutan funcionamiento de los equipos, contemplando las posibilidades de daños a nivel tanto de hardware como de software.

Por otra parte, conocer previamente cuando se va a generar un fallo es muy difícil, ya que en la mayoría de veces, sólo se sabe que hay problemas cuando se observan comportamientos extraños en el sistema. Ante esto, el mantenimiento a nivel de software se basa ante todo, en mantener el software con las actualizaciones de seguridad recomendadas por los desarrolladores, además de realizar labores de limpieza de archivos y usuarios no activos, pero sólo cuando se considere prudente y necesario hacerlo, entre otras tareas que son importantes para que el sistema se mantenga funcionando adecuadamente y evitando que a futuro el sistema sufra fallas, sobre todo de seguridad, a causa de esto.

En cuanto al mantenimiento correctivo, dado a que los equipos son nuevos, en estos momentos su funcionamiento es óptimo, tanto a nivel de hardware como de software, pero se han analizado, a futuro las posibles fallas que se pueden presentar de forma imprevista, en los que se analizan los fallos en función los alcances que pueden llegar a tener los administradores para solucionarlos; ya que pueden existir casos en los que se necesite apoyo técnico, especialmente, en casos de problemas o daños a nivel de hardware.

3.6 ADMINISTRACIÓN DEL CLÚSTER DE ALTA DISPONIBILIDAD

El clúster de alta disponibilidad, al estar compuesto por un conjunto de herramientas software, debe configurarse de manera adecuada para que todo el software realice su labor de manera correcta. Para esto, se cuenta con la interfaz de línea de comandos CRM (Cluster Resource Manager), con el cual se pueden gestionar los recursos y generar órdenes para el software de alta disponibilidad.

Aunque el CRM provee los comandos necesarios para el manejo general del clúster, puede llegar a ser muy extensa y complicada la configuración desde línea de comandos, lo que haría poco eficiente la tarea de administración y configuración. Ante esto, se ha optado por utilizar un GUI de Java llamado LCMC (Linux Cluster Managemente Console), su interfaz de inicio se muestra en la figura 16.

LCMC provee una interfaz amigable con la cual se puede gestionar remotamente todo lo relacionado con el clúster, de una forma gráfica y más practica que la interfaz de líneas de comandos CRM. LCMC hace uso del protocolo SSH para realizar la conexión, dándole una buena característica de seguridad en este aspecto e interactúa adecuadamente con Pacemaker, DRBD y demás software del clúster.

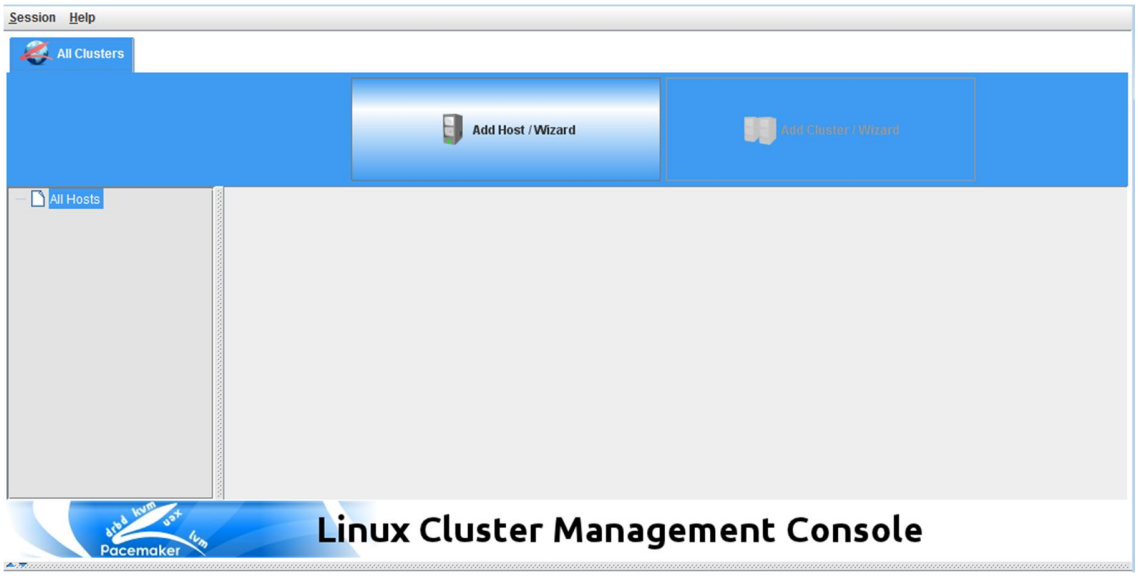

Figura 16 Interfaz de inicio del GUI de Java LCMC versión 1.0.2

La labor de administración del clúster, es una actividad que incluye tareas como el montaje y la puesta a punto de servicios que se desean tener en alta disponibilidad, actividades de monitoreo y formas de respuesta ante eventos no

esperados. Todo lo anterior, se condensa en las actividades de gestión en las cuales se debe velar por mantener una infraestructura óptima del clúster.

Además de la gestión del clúster a través del LCMC, la labor administrativa se complementa con la revisión de los registros (Logs) del sistema generados por la actividad del software de manejo de la alta disponibilidad; de esta forma, se puede actuar de manera oportuna ante cualquier anormalidad que se pueda llegar a presentar en la actividad cotidiana en los equipos servidores.

4. NORMATIVIDAD

En su conjunto, toda actividad realizada dentro de los equipos servidores, debe estar regida bajo una serie de normativas que representen concretamente los alcances y las restricciones de su uso y gestión, conservando de esta forma un control administrativo integral. Es decir, tanto administradores como demás usuarios del sistema, deben tener conciencia de los alcances y limitaciones de su actividad en los equipos.

En general, lo que se busca con la creación de políticas o normas, es propiciar principalmente un entorno de trabajo organizado, buscando ante todo un uso adecuado de los recursos informáticos, para que de esta forma, se genere un ambiente controlado con sentido de la responsabilidad. Con esto, se pretende que se adecúe fácilmente el uso de las máquinas a los cambios administrativos, pues los equipos son administrados por estudiantes de la Escuela de Ingeniería de Sistemas que al finalizar sus ciclos académicos, delegan la labor a nuevos administradores.

Dado a que la labor fundamental de dichos equipos es de tipo académico e investigativo, implica que a éstos tendrán acceso diferentes tipos de usuarios, tanto para acceso a servicios, como a desarrollo de sus trabajos de grado. Las normas de seguridad, se han creado en torno a dos aspectos básicos fundamentales, el primero es desde las normativas que rigen a los administradores y usuarios que desarrollan e investigan apoyándose en el uso de los equipos y el segundo en cuanto a la seguridad del equipo, los cuales son profundizados a continuación.

4.1 NORMAS DE USUARIOS Y ADMINISTRADORES

Los procesos administrativos son los que tienen el mayor impacto en el comportamiento y funcionamiento adecuado del sistema y la seguridad del mismo,

por tanto poseer y conocer lineamientos básicos para la realización de dicha labor administrativa es fundamental, ya que si en dado caso, no se siguiera una serie de normas para la realización de cierta actividad administrativa, podría ponerse en riesgo el sistema mismo. Las normas fundamentales que rigen a los administradores se encuentran dentro de los siguientes grupos principales:

- Preservar la confidencialidad de la información sensible de acceso a los equipos.
- Dar soporte a usuarios que requieran uso de los equipos.
- Conocer y poner en práctica los lineamientos establecidos en el manual de administración.

En cuanto a los demás usuarios que tienen acceso a los equipos, se ha establecido una serie de normas de uso de los recursos de los equipos, que les darán a conocer por parte del administrador, indicándoles claramente sus alcances y las limitaciones. Dentro de las principales normas se encuentran:

- Utilizar sólo los equipos con fines académicos y de investigación.
- Es responsabilidad de los usuarios los tipos de contenidos publicados en los servicios web que instalen en los equipos y de su visibilidad a través de los dominios sistemas.uis.edu.co y delfin.uis.edu.co, mediante el anexo de un documento de compromiso firmado por los estudiantes y demás usuarios que lo requieran.
- Los desarrolladores deben buscar limitar el uso de funciones y de piezas de código que puedan representar riesgos de exploits de desbordamiento de memoria o que generen riesgos en los accesos a bases de datos.
- Aceptar las limitaciones en cuanto a la cantidad de privilegios dentro del sistema y de acceso a directorios asignados.
- En caso de requerir privilegios para el desarrollo de sus trabajos más allá de los asignados, comunicarlos concretamente al administrador para evaluar el caso.

- Seguir las instrucciones y recomendaciones dadas por parte del administrador para el acceso y uso de los recursos asignados para el desarrollo de su trabajo.

4.2 POLÍTICAS DE SEGURIDAD

Definidas las normas, tanto para los usuarios desarrolladores como para los administrativos, se debe estructurar una serie lineamientos con los cuales toda actividad hecha en los servidores se encuentre bajo los parámetros de uso establecidos anteriormente. De igual manera, se debe plantear algunos escenarios en los cuales se contemplen los riesgos, las amenazas, la posibilidad de daño total de las máquinas y cómo se debe actuar ante esto, entre otros, con el fin de contar con procedimientos claros, que permitan hacer tales labores de manera organizada, reaccionando oportunamente ante posibles peligros o daños por medio de la normatividad planteada.

Todos los aspectos contemplados en las políticas de seguridad se encuentran establecidos bajo los siguientes criterios:

- Gestión de Usuarios y contraseñas.
- Normas de Administración.
- Manejo de respaldos de los sitios web.
- Gestión de Riesgos.

Las políticas se encuentran explícitas bajo regulación interna administrativa.

5. MODELO DE ADMINISTRATIVO

Un modelo es una representación gráfica o conceptual de una realidad que se desea representar; se señala que se modela *"una realidad"*, porque el objeto de estudio (lo que se desea modelar) es sólo una parte de lo que se considera realidad o una visión de esa realidad, pues cada persona o grupo de personas puede interpretar lo que percibe del entorno de formas diferentes y con variado nivel de detalle. De manera global, se puede decir que a partir de conocimientos previos y de modelos, sean estos formales o no, las personas y las organizaciones condicionan sus conductas, estrategias y en general, su interacción con el ambiente.

Es por esto que el planteamiento de un modelo desde la perspectiva administrativa, dentro de la planeación misma del proyecto realizado, corresponde a un aspecto muy importante dentro del planeación de la oferta y creación de servicios orientados desde una perspectiva organizacional; ya que a partir de un modelo de administración, puede posibilitarse una gestión organizada de los diferentes recursos informáticos y los servicios prestados, pues en éste, puede representarse los diferentes procesos organizacionales y los entes implicados en tales procesos.

5.1 PLANTEAMIENTOS INICIALES

Al pretenderse representar la idea de prestación y desarrollo de servicios web en la Escuela de Ingeniería de Sistemas desde los equipos servidores Sistemas y Delfín a través de un modelo administrativo, se ha delimitado en primera instancia el propósito mismo de los servicios prestados, a qué y a quienes van orientados, y en general, los sectores que de una forma u otra interactúan con el desarrollo, gestión y uso de los servicios, comprendiendo todos estos procesos y elementos desde una perspectiva organizacional. Se ha decidido visualizarse como una organización, porque es desde esta óptica en la cual los grupos de personas

implicados pueden realizar su labor de una manera clara, ordenada y dentro de los límites establecidos, pues cada quien puede saber lo que puede y debe hacer en un momento determinado.

De igual manera, es de saberse que desde una visión organizacional, toda la estructura funcional se encuentra sujeta a cambios, dado a que el entorno mismo y las tendencias tecnológicas se crean y evolucionan constantemente. Entonces, tales cambios a nivel interno, pueden abordarse por medio del planteamiento de escenarios dinámicos, en los cuales se aborden diferentes variantes que puedan afectar la labor funcional de la organización, en este punto, las reglas de gestión de los diferentes procesos desempeñan un papel crucial para el logro de una identidad organizacional, con la cual tales planes de acción cumplan su labor de manera satisfactoria en las labores cotidianas y en las que se harán a futuro.

Ya enfocados en el contexto organizacional, el siguiente paso es buscar una manera de diseñar un modelo que contemple los procesos de creación y desarrollo de servicios y las formas como la administración interviene en estos. Para esto, se llevó a cabo un proceso de investigación y análisis donde se tomó la decisión de crear un modelo en el cual se tenga en cuenta:

- La normatividad de uso y administración de los servidores.
- La labor administrativa y sus diferentes canales de comunicación.
- La labor de los desarrolladores de los servicios en relación al uso de los equipos servidores.
- La interacción de los servicios ofrecidos con el entorno académico de la Escuela de Ingeniería de Sistemas y la Universidad Industrial de Santander.
- Planeación y desarrollo de nuevos servicios.

Para agrupar todas las anteriores condiciones en un solo modelo se tomó la decisión de implementar un diseño que contemple la administración como una parte funcional de la organización misma; ya que todo proceso de gestión, ya sea

de recursos físicos, software, entre otros, que posibilitan el cumplimiento de la labor organizacional (desarrollo y oferta de servicios web en la Escuela de Ingeniería de Sistemas) no deben ser independientes de la organización misma, por tanto, debe buscarse una forma de considerar tales aspectos en el modelo a realizar.

Una manera de modelar la administración como una función de la organización y teniendo en cuenta todo lo anteriormente planteado, es el diseño mediante el enfoque sistémico del modelo de sistema viable. En esta metodología de modelado, que fue propuesta por Stafford Beer, se trabaja con la idea de interpretar los sistemas sociales humanos como organismos vivos, los cuales tiene sistemas internos que interactúan y realimentan, propiciando que éste se adapte a un ambiente cambiante.

Cabe señalar, para que el modelo a diseñar se considere un Sistema Viable, debe considerarse aspectos tales como:

- La organización debe ser comprendida como un sistema, que cuente con niveles o subsistemas que se auto-regulan y con capacidad de decidir el momento y la forma en que realiza su acción.
- La administración no es centralizada, por lo tanto, cada nivel es considerado autónomo y debe generar respuesta o salidas hacia otros subsistemas de la organización, para que de esta manera se haga posible su gestión.
- En el modelo, la organización se debe considerar como un todo funcional, mayor a la suma de sus partes, con lo que los subsistemas deben contar con entradas, salidas y medios de realimentación de la información.
- La organización no es independiente del entorno en el que se encuentra y debe contar con medios que le permitan adaptarse a los cambios de éste.

- Se debe tener claro el límite organizacional del sistema, es decir, debe tener claramente definidas las actividades fundamentales (el propósito de la organización) para su adecuada administración.
- Aplicación de mecanismos para control de variedad (cantidad de información que pasa de un subsistema a otro).

Con un vistazo general de los anteriores planteamientos puede llegarse a comprender la relevancia de la creación de un modelo que represente funcionalmente la organización, que consecuentemente proporciona los medios para generar una buena estructura de trabajo, logrando optimizar la función administrativa y sus canales de comunicación y en general poder contemplar de una forma sencilla la organización misma, las funciones, los procesos y cómo estos interactúan.

5.2 ACERCA DEL MODELO DE SISTEMA VIABLE

El modelo de sistema viable fue desarrollado por Stafford Beer y fue explicado en varias de sus obras. En este tipo de modelos se consideran mecanismo de regulación y división en subsistemas para que la organización se adapte a su entorno y por tanto la administración se haga de una manera dinámica y efectiva.

Los sistemas viables están compuestos por cinco subsistemas que interactúan entre ellos. En la figura 17, se representa una visión general de la estructura básica del Modelo de Sistema Viable (Beer S, 1981) y a continuación, se detalla cada componente y su función dentro del modelo.

Sistema Uno: Es el subsistema en el cual se realizan las operaciones primarias de la organización, como lo son la producción de bienes o servicios. Cada sistema uno se encuentra en un entorno específico o entorno propio, visible en la figura 17.

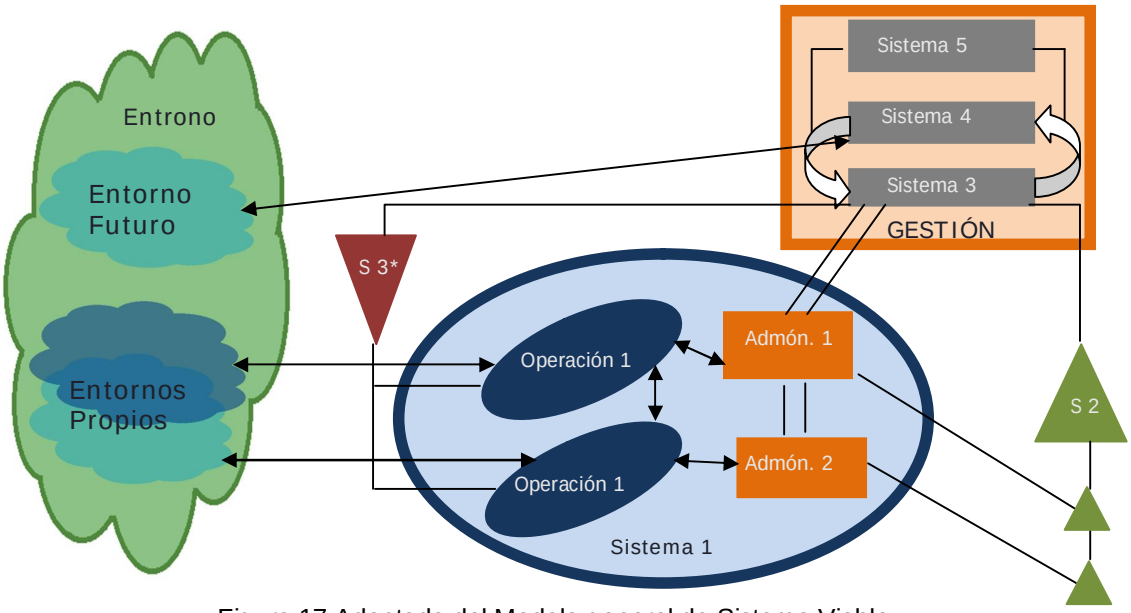

Figura 17 Adaptado del Modelo general de Sistema Viable

Sistema Dos: Representa los canales de manejo de la información acerca de las operaciones realizadas en el sistema uno. Este opera en el dominio administrativo y provee de información importante acerca de la operaciones del sistema uno al sistema tres, con lo cual la administración logra regular las actividades realizadas en el sistema uno.

Sistema Tres: Es el encargado de generar las diferentes estructuras de control que propician un ambiente interno estable, tales como reglas, derechos y responsabilidades del sistema uno que son monitoreadas desde el sistema tres*. Además, el sistema tres provee un canal entre las operaciones de los sistemas cuatro y cinco.

Sistema Tres*: Representa el canal de monitoreo de las operaciones del sistema uno desde el sistema tres, tal información puede ser utilizada por los sistemas cuatro y cinco para la toma de decisiones.

Sistema Cuatro: Es el encargado de generar escenarios en los cuales se pueda evaluar la organización a futuro; esto se representa relacionado con un entorno futuro, pues en este sistema se crea un contexto en el cual se pueda responder a los cambios en el entorno adecuadamente y a los retos y oportunidades que estos representan.

Sistema cinco: Es el encargado de establecer las políticas y la toma de decisiones final. Debe facilitar un ambiente de interacción en el cual los sistemas tres y cuatro puedan llegar a acuerdos que favorezcan el normal desarrollo de las actividades de la organización.

En este modelo todas las actividades organizacionales se realizan dentro de un entorno y la organización misma no se debe considerar aislada de dicho entorno, de allí que este modelo presenta una forma de pensar la administración dinámica y con capacidad de adaptación a los cambios.

Las líneas que conectan las diferentes partes del modelo están sujetas a la **ley de variedad requerida** para el establecimiento de un sistema de control, la cual cuenta con filtros para que el flujo de información del sistema más general sea tomado por el más particular y amplificadores para la comunicación del más particular al más general. De esta forma se puede lograr una comunicación más efectiva y un equilibrio natural entre los diferentes sistemas de la organización, por ejemplo, los datos que fluyen desde las operaciones a la administración son filtrados para que este último pueda tomar los datos fundamentales para la toma de decisiones sobre las operaciones, así mismo, la información que fluye desde la administración a las operaciones cuenta con amplificación para que a partir de tales decisiones se realicen las diferentes operaciones.

5.3 DESARROLLO DEL MODELO DE ADMINISTRACIÓN

A partir de la base teórica, y del proceso administrativo que se ha llevado a cabo durante el desarrollo del presente proyecto, se ha ido construyendo el modelo administrativo organizacional, en el cual se ha ido condensando la forma de trabajo que se lleva a cabo cotidianamente en el grupo.

El modelo de sistema viable diseñado en torno al ambiente organizativo de los servicios ofrecidos y desarrollados en los servidores sistemas y delfín pertenecientes a la Escuela de Ingeniería de Sistemas, tiene como propósito fundamental plasmar una forma de administración que tenga en cuenta los diferentes aspectos funcionales, las normas y demás formas de regulación, que contribuyen a un uso adecuando de los equipos.

Para plantear el modelo se ha revisado los diferentes subsistemas presentes en la organización para relacionarlos según el modelo de sistema viable. Igualmente, se ha delimitado el ambiente en que desarrolla sus actividades la organización, sus diferentes aspectos funcionales, los canales de comunicación el entorno y los entornos propios, así:

Entorno Relevante.

Es la Escuela de Ingeniería de Sistemas, los desarrolladores y los servicios hacen parte de esta escuela. En el modelo de sistema viable, se destaca que las fronteras del entorno relevante son borrosas, por tanto, el entrono es graficado de manera irregular, ya que este es cambiante. Para este caso, se puede decir que los servicios desarrollados pueden ser ofrecidos a un entorno más allá de las fronteras delimitadas, es decir, más allá de la EISI, pero sujetos a sus normas misionales.

Sistema Uno.

En este caso, las tareas primarias son el desarrollo y ofrecimiento de servicios orientados a la web. Como todas las operaciones, de lo que se considera sistema uno, son desarrolladas dentro de un ambiente propio (En la figura 18, forma irregular color azul oscuro), para este caso tal entorno en el que se desarrollan las operaciones son los servidores sistemas y delfín, ya que son estos equipos en los que se prueban los proyectos en desarrollo y se alojan los servicios ofrecidos. Es de resaltar que todos los servicios alojados en los servidores sistemas y delfín no son de uso comercial, pues se encuentran en un ambiente académico.

Todas las operaciones realizadas deben tener un medio de regulación, es decir, debe existir una coordinación de proyecto, desde la cual se hagan los procesos de planeación y toma de decisiones para la orientación adecuada del proceso de desarrollo o administración del servicio web y éste no se desvíe del propósito principal.

Como se observa en la figura 18, dentro del óvalo principal (azul claro) que enmarca las operaciones, la actividad de administración de los procesos, es llevada a cabo tanto por los directores de proyecto como de los estudiantes que desarrollan el proyecto, pues es una actividad conjunta en la que ellos interactúan intercambiando ideas y tomado las decisiones que consideren adecuadas para que el servicio web cumpla con los objetivos planteados; de igual manera, las actividades realizadas en este nivel son reguladas por otros subsistemas.

Sistema Dos.

Es el canal de de comunicación entre los Administradores de los recursos informáticos y los administradores de los servicios (representado en el triángulo verde). Este es un subsistema muy crítico, porque es en este punto donde se establecen las pautas para la realización de tareas dentro de los servidores, luego, según sea la normatividad establecida (Flecha descendente del cuadro naranja claro al óvalo azul celeste) se llegan a acuerdos de uso y los administradores de

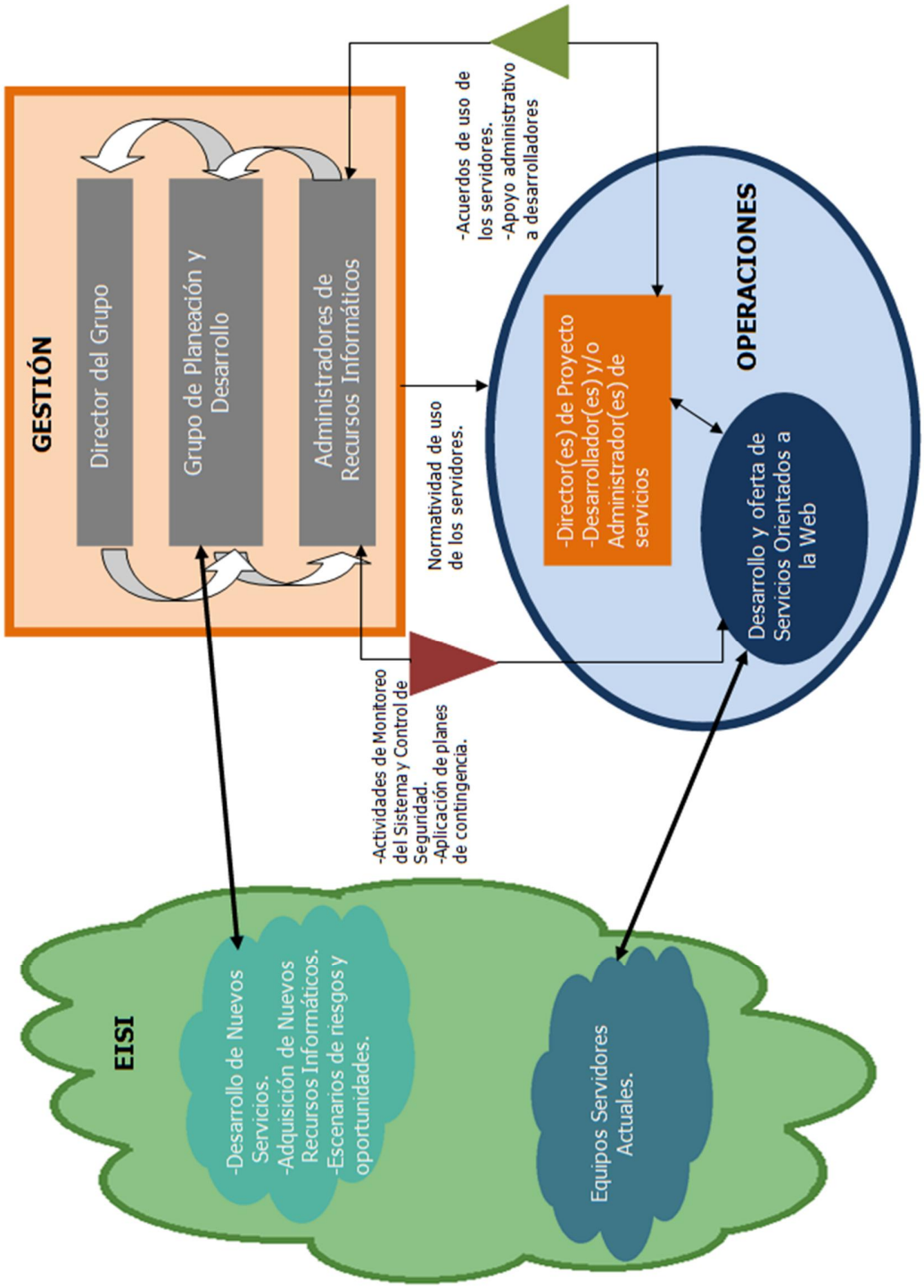

Figura 18 Modelo de Sistema Viable para la gestión de servicios en los equipos Sistemas y Delfín

los equipos pueden brindar soporte para la realización de ciertas tareas, para que los servicios principalmente se ofrezcan a la comunidad académica sin mayores contratiempos.

Sistema Tres.

Este subsistema se encuentra representado por la administración de los recursos informáticos, ya que sirve como medio entre los demás miembros del grupo de gestión principal (representado en el rectángulo naranja claro), y los que gestionan las operaciones, su canal de comunicación es el sistema dos, con lo cual se mantiene regulado el sistema organizacional y se pueden desempeñar todas las operaciones con autonomía pero acogiéndose a los acuerdos normativos establecidos. Los administradores de los servidores, son los que poseen el control principal de los equipos, por tanto generan la normatividad de uso y los planes de contingencia para los equipos a partir de la orientación y el consenso de ideas con los otros miembros del grupo de gestión.

Sistema Tres*.

Es un sistema de apoyo para los administradores de recursos informáticos, donde (representado en el triangulo rojo oscuro) se establecen las actividades de monitoreo, en el cual se busca garantizar que las operaciones hechas se encuentren dentro de los parámetros de uso establecidos. En este sistema está el monitoreo a través de los registros de sistema de los servidores y aplicación de los planes de contingencia, por si se presentan problemas o fallos en los equipos por diferentes razones, que pueden ser independientes a las actividades operacionales, y así pueda actuarse de manera oportuna y afectar lo menos posible la prestación y desarrollo de los servicios.

Sistema Cuatro.

Es un grupo de planeación, en este se encuentran los directores de proyectos, que puede ser el director del grupo, y los estudiantes que están dispuestos a

desarrollar tales proyectos planeados. Así mismo, la planeación no se limita sólo a crear escenarios en los cuales se puedan desarrollar nuevos servicios, sino en la medida que se disponga de nuevos equipos informáticos, tanto el director del grupo como los administradores, pueden planear su uso a futuro de la mejor manera posible, planteando en cada caso escenarios de riesgos y oportunidades que se puedan presentar e ir generando planes de contingencia según sea el caso evaluado. Por tanto, en este grupo de planeación, interactúan tanto directores, administradores y desarrolladores para adaptarse a las condiciones y retos que se presenten con el paso del tiempo. En este sistema al ser de visión hacia futuro, se representa conectado a un entorno futuro (forma irregular de color azul claro), lo cual indica que la actividad de planeación se encuentra sujeta a cambios en el entorno actual.

Sistema Cinco.

En este se encuentra el director del grupo, su actividad principal gira en torno a la toma de decisiones finales, de acuerdo a la información que se le suministra desde los demás subsistemas. Además, el director al ser un miembro activo de la EISI, también puede ser director de proyectos y tener contacto directo en el sistema de operación (sistema uno), por tanto, puede actuar en diferentes campos administrativos según le sea requerido.

5.4 PLANTEAMIENTO DE MECANISMOS DE REGULACIÓN

Para que el modelo planteado anteriormente se considere un sistema viable, los canales de comunicación deben encontrarse auto-regulados para tener una comunicación efectiva, de acuerdo a la ley de variedad requerida mencionada en la sección 5.2. El diseño de los filtros y los amplificadores en las líneas de comunicación se realizó de acuerdo a criterios administrativos de manejo de información de manera equilibrada, por ejemplo, como no toda la información del entorno debe ser trasmitida al grupo de operaciones, estos deben contar con criterios de selección de la información para captar sólo la que necesita, de igual

manera la administración maneja todos los procesos de la parte operativa, así debe contar con los medios para que sus propuestas lleguen amplificadas al contexto de desarrollo y administración de manera adecuada. Estos criterios se encuentran representados en la figura mostrada a continuación.

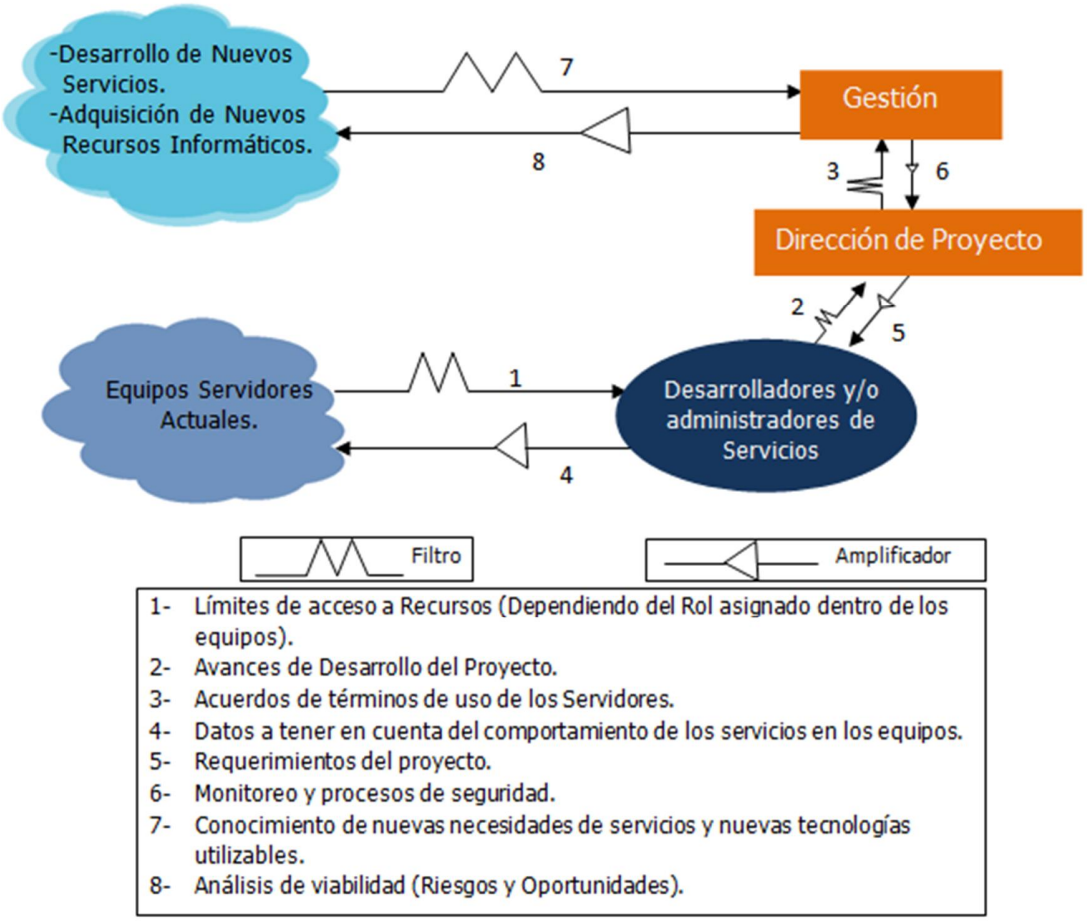

Figura 19 Sistema de regulación de la comunicación

Como se observa en la anterior gráfica, la comunicación entre las partes se encuentra basada en procesos de filtrado y amplificación según sea el rol desempeñado; de igual forma, en la tabla inferior, se presenta el regulador implementado para cada línea de comunicación. Con la creación de estos mecanismos de comunicación, se busca generar estabilidad general en el ambiente de trabajo, lo cual determina la efectividad en todos los procesos desarrollados en el grupo.

En general, la creación del modelo se hace con un propósito administrativo, en el cual, se pretende plasmar una forma de gestión de los recursos informáticos dentro de un contexto organizacional, asignando roles a los diferentes actores que interactúan con los servidores sistemas y delfín. Su desarrollo se realizó de manera constante, a medida que se avanzaba en la configuración y administración de las máquinas, del conocimiento del entorno de producción y los procesos de investigación respectivos.

CONCLUSIONES

- El proceso administrativo, no se limita a la instalación de herramientas software y a la realización de tareas de monitoreo de dichas aplicaciones, es una tarea global, que involucra los diferentes aspectos funcionales desde el hardware hasta la prestación de servicios, incluyendo la automatización de tareas administrativas básicas y la realización de una normativa de gestión.
- Como resultado de la investigación, se logró implementar de manera exitosa, un clúster de alta disponibilidad; mediante el uso de herramientas de software libre, generando unos servicios computacionales confiables para su uso en la Escuela de Ingeniería de Sistemas y la comunidad académica en general.
- Con el apoyo de tecnologías de software libre para la alta disponibilidad, se logra mantener la información crítica fuera de un punto simple de fallo, donde no sólo la información se mantiene redundante, sino también el enlace de comunicación de los equipos, de esta forma, la prestación de los servicios no se ve alterada por algún evento inesperado en uno de los servidores.
- El diseño de un modelo de administración desde una perspectiva sistémica organizacional, apoya la gestión de los recursos, ya que esboza las formas de comunicación entre todos los que hacen uso de los equipos, contemplando las diferentes formas de regulación de las actividades, su monitoreo y la planeación de nuevas formas de uso de dichos servidores para la adaptación a cambios.
- Con la realización del presente proyecto, se logró afianzar los conocimientos fundamentales de la carrera, teniendo en esta experiencia la oportunidad de realizar una especialización en administración de servidores y manejo de tecnologías de alta disponibilidad, mediante el aprendizaje durante el proceso investigativo.

RECOMENDACIONES

- El propósito del entrenamiento de los relevos, es dar a conocer a éstos las diferentes actividades que deben realizar, mostrándoles la forma de trabajo que es llevada a cabo en el grupo, evitando inconvenientes a futuro. Por tanto, este proceso de entrenamiento debe ser constante en cada uno de los proyectos subsiguientes relacionados a la labor administrativa.
- El software instalado al ser de carácter libre, se encuentra sujeto a permanentes actualizaciones lanzadas por las comunidades de desarrolladores, por tanto, es fundamental evaluar la viabilidad de la instalación de las mismas, para evitar afectaciones en la operatividad y prestación de servicios.
- Para futuras incorporaciones de equipos en el clúster, se debe tener en cuenta los diferentes lineamientos de seguridad, para que de esta manera, se minimicen los riesgos que se puedan presentar durante el proceso de expansión.
- Como se mencionó durante el desarrollo del presente proyecto, el manejo de software libre representa una opción muy conveniente para el montaje de infraestructuras de servicios seguras y estables; por tanto, es importante mantener el uso prioritario de herramientas de carácter libre para posteriores instalaciones en los equipos.

BIBLIOGRAFÍA

- Barisani A, Bader T, Biles S, Clark C, Chiesa R, Endres P, Feist R, Ghirardini A, Ho J, Ivaldi M, Lavigne D, Presti S, Low C, Miller T, Puccetti A. *Hacking Exposed Linux: Linux Security Secrects & Solutions*. 3rd ed. ISECOM, McGraw-Hill, 2008.
- Nemeth E, Snyder G, Hein T, Whaley B. *Unix and Linux Systems Administration Handbook*. 4th ed. Pearson Education, Inc., 2011.
- Andrade H, Dyner I, Espinosa A, López H, Sotaquirá R. *Pensamiento sistémico: Diversidad en búsqueda de Unidad.* Ed. Universidad Industrial de Santander, 2001
- Espejo R. *Conceptos y Prácticas de control; Una experiencia concreta: La dirección industrial en Chile.* Corfo, Santiago de Chile, 1973.
- Beer S. *Brain of the Firm.* 2nd ed, Chichester Wiley, London, 1981
- Sitio web de la comunidad Debian. [Online]. Disponible: http://www.debian.org/
- Sitio web de la comunidad desarrolladora de Apache. [Online]. Disponible: http://www.apache.org/
- Sitio web de la comunidad desarrolladora de Apache Tomcat. [Online]. Disponible: http:tomcat.apache.org/
- Sitio web del equipo de desarrolladores PHP. [Online]. Disponible: http://www.php.net/
- Sitio web de MySQL. [Online]. Disponible: http://www.mysql.com/
- Sitio web del proyecto Postfix. [Online]. Disponible: http://www.postfix.org/
- Sitio web del proyecto CyrusIMAP. [Online]. Disponible: http://www.cyrusimap.org/
- Configuración de un servidor de correo con Postfix y Cyrus. [Online]. Disponible: http://www. Linuxsilo.net/

- Sitio web del proyecto SquirrelMail. [Online]. Disponible: http://www.squirrelmail.org/
- Sitio web de la comunidad Linalco. [Online]. Disponible: http://www.linalco.com/
- Sitio web de la comunidad de desarrollo clusterlabs. [Online]. Disponible: http://www.clusterlabs.org/
- (2008) Sitio web del proyecto DRBD de la comunidad linbit. [Online]. Disponible: http://www.drbd.org/
- (2007) Sitio web del proyecto Openais. [Online]. Disponible: http://www.openais.org/
- (2008) Sitio web del proyecto Corosync. [Online]. Disponible: http://www.corosync.org/

ANEXO 1: ARTÍCULO

Modelo administrativo para gestión de servidores Linux, implementando mecanismos de seguridad y tecnologías de software libre orientadas a la Alta Disponibilidad.

MANUEL GUILLERMO FLÓREZ BECERRA
M.Sc en informática. Universidad Industrial de Santander
mgflorez@uis.edu.co

ALEXANDER BARBOSA AYALA
Ingeniero de Sistemas. Universidad Industrial de Santander
alexanderbarbosaayala@gmail.com

ELKIN DARÍO MUÑOZ DUARTE
Ingeniero de Sistemas. Universidad Industrial de Santander
elkin.dmd@gmail.com

RESUMEN

En este artículo se describe el proceso administrativo en servidores Linux, con base a la implementación de mecanismos de seguridad para la integridad y manejo de los recursos informáticos, desde una perspectiva administrativa organizacional y usando procedimientos basados en tecnologías de software libre orientadas a la alta disponibilidad.

PALABRAS CLAVE: administración, alta disponibilidad, backup, clúster, corosync/OpenAIS, DRBD, pacemaker, CRM

ABSTRACT

This article describes the administrative process in linux's servers, based on the implementation of safety mechanism for the integrity and handling of informatics resources, from an organizational administrative perspective and using procedures based on free software technology oriented to high availability.

KEYWORDS: administration, backup, clúster, corosync/OpenAIS, DRBD, high availability, pacemaker, CRM.

1. INTRODUCCIÓN.

La administración de servidores es una labor que con el tiempo se hace cada vez más compleja a medida que las organizaciones crecen, al igual que sus componentes hardware y software. Es necesaria una visión a nivel organizacional para realizar una administración consolidada mediante la implementación de herramientas especializadas que tengan en cuenta la seguridad e integridad de la información, los mecanismos de control adecuados y la administración eficiente de recursos informáticos.

Los clústeres son una tecnología comúnmente aplicada para diferentes propósitos dependiendo de la actividad computacional a realizar; básicamente es un conjunto de computadoras que usan componentes de hardware comunes y presentan un comportamiento de unidad simulando un ambiente de una sola computadora.

En la EISI (Escuela de Ingeniería de Sistemas e Informática) de la UIS (Universidad Industrial de Santander) se dispone de servidores y servicios para un entorno educativo, de profesores, estudiantes y comunidad académica que requiere de estos servicios en forma continua y permanente.

Al combinar la gestión administrativa con tecnologías orientadas a la alta disponibilidad y seguridad, es posible generar un ambiente confiable para satisfacer estos requerimientos de servicios académicos.

2. MARCO TEORICO

2.1 Clúster

La evolución del clúster, según sus usos, comprende desde la programación distribuida hasta la implementación de servicios en un entorno de alta disponibilidad [1].

Los servicios provistos de acuerdo a la orientación de la organización son:

- Alto rendimiento (High Performance Computing Clúster, HPCC), proveer un gran rendimiento a nivel de la velocidad en que se procesan los datos [2].
- Alta disponibilidad (High Availability, HA), establecer una infraestructura donde se mantengan

los servicios de manera permanente independientemente de la caída de nodos [3].

- Balanceo de carga (Load Balancing), distribuir la carga de los diferentes elementos computacionales en una red de trabajo, mediante un balanceador de carga (Load Balancer) [4].

La composición de un clúster viene dada por los siguientes elementos:

- Nodos
- Sistema operativo instalado
- Protocolos de comunicación
- Servicios a disponer
- Dispositivos de almacenamiento
- Aplicaciones para el entorno del clúster
- Middleware, para establecer comunicación entre las diferentes aplicaciones que conforman el clúster.

2.2 Sistemas Operativo Debian

Es una distribución Linux, coherente a la filosofía del núcleo Linux y de GNU bajo licencia GPL (General Public Licence), la versión 6 fue lanzada el 6 de febrero de 2011 [5] y ha sido seleccionada como SO (Sistema Operativo) base para la implementación de la alta disponibilidad, no solo por ser uno de los sistemas operativos más utilizados en el mundo como servidor web [6], sino también por ser estable, versátil a nivel de mantenimiento e instalación de herramientas, bajo consumo de recursos, gran soporte y documentación.

2.3 Clúster de Alta Disponibilidad

Para mantener los servicios y la información crítica fuera de un punto único de fallo SPOF (Single Point Of Failure), es necesario la implementación de un clúster de alta disponibilidad; estos son agrupaciones de dos o más servidores que trabajan simultáneamente compartiendo información y servicios tales como el servidor web *Apache*, el gestor de base de datos *MySQL*, sistemas de ficheros, sitios web y otros, existiendo una comunicación permanente entre los servidores que permite reaccionar ante cualquier evento imprevisto [7], mediante una infraestructura de elementos redundantes, como volúmenes compartidos y configuración de interfaces de red extra.

2.4 DRBD (Distributed Replicated Block Device)

El DRBD es una herramienta bajo licencia GPL que permite la duplicación de un dispositivo a través de una red asignada para apoyo de clústeres de alta disponibilidad [8].

Cada uno de los componentes instanciados presenta un rol primario o secundario; el primario puede ser usado sin restricciones de lectura y escritura a diferencia del secundario que no tiene acceso completo, para mantener la coherencia en el caché.

2.5 Corosync/OpenAIS

OpenAIS, es un software con licencia Open Source, hecho con el fin de proveer una interfaz de clúster a nivel de mensajería basándose en el estándar de alta disponibilidad AIS (Application interface Specification) [9]; AIS es un API (Application Programming Interface), para el sistema de comunicación en el clúster, mediante el uso de middleware y aplicaciones de servicio [10]; Corosync además de proveer un sistema de comunicación presenta características adicionales de sincronía virtual, reinicio de procesos, configuración y estadísticas en una base de datos y un sistema de agrupación de aplicaciones [11].

2.6 Pacemaker

Es un software bajo licencia GPL para la gestión de los servicios del clúster de alta disponibilidad, con el apoyo de la infraestructura de clúster que se asigne (Corosync/OpenAIS o Heartbeat), logra proveer una interfaz para la detección y recuperación de los nodos ante cualquier fallo a nivel de recursos [12].

3. ALTA DISPONIBILIDAD

3.1 Servicios disponibles

En la EISI mediante el clúster de alta disponibilidad y apoyados en las herramientas Apache [13], Mysql [14], Tomcat (módulo para paginas dinámica con contenidos Java) [15], PHP (Hypertext Pre-processor) [16] y JAVA [17] se proveen diversos servicios como: Aulas virtuales para docentes y alumnos (MeiWeb y Moodle), bases de datos, sitios web para estudiantes realizando proyecto de grado, además, se proyecta ofrecer a la comunidad académica servicios de computación en la nube mediante maquinas virtuales implementadas sobre el clúster.

3.2 Configuración

Un clúster de alta disponibilidad tiene diferentes modalidades de infraestructura: *N+1*, *N a N*, *Split-site*; *Activo/Pasivo*; en esta última, uno de los nodos mantiene los servicios y los sistemas de archivos compartidos y el otro se mantiene las réplicas en espera ante un caso de fallo. Para la creación del clúster se usaron dos servidores y previo a un estudio, se seleccionó el software *DRBD*, *Pacemaker* y *Corosync/OpenAIS* para conformar el stack de aplicaciones de alta disponibilidad. La Figura 1 muestra la infraestructura planteada y la manera como se encuentra configurado el clúster de alta disponibilidad para el entorno de trabajo.

Las anteriores herramientas, en conjunto, permiten el funcionamiento del clúster de alta disponibilidad; los siguientes parámetros deben considerarse para el montaje del clúster:

- Entre los nodos debe existir un enlace de red redundante debidamente configurado.
- El archivo */etc/network/interfaces* debe configurarse incluyendo una sub-interfaz de red con una dirección IP que pertenezca a la misma

red del enlace redundante, donde se apoya el clúster para la comunicación entre nodos.

- El servicio de *corosync* debe estar configurado, para que se inicialice ante un reinicio del sistema.
- La llave de autenticación de corosync, generada en uno de los nodos, se envía por el protocolo de comunicación *SSH* hacia el otro nodo.
- El archivo de configuración de corosync, en ambos nodos, debe tener en la opción *bindnetaddr*, la dirección de red para los ajustes configurados en la interfaz redundante.
- Deshabilitar la propiedad *stonith*, dentro del clúster de alta disponibilidad, para no delimitar el uso de los servicios en los nodos. a nivel de los nodos implementados [18].
- Crear el sistema de ficheros para el volumen que se dispondrá en modo espejo, teniendo en cuenta, que en el nodo esclavo debe existir otro volumen con la misma capacidad.
- Instanciar de manera correcta el recurso para *DRBD*, especificando para cada uno de los host el dispositivo, el disco, el socket y los metadatos.
- Uso del *CRM* (Cluster Resource Manager) para configuración de cada uno de los servicios a disponer en el clúster de alta disponibilidad, entre los que se resaltan, el sistema de archivos, la base de datos y el servidor web.

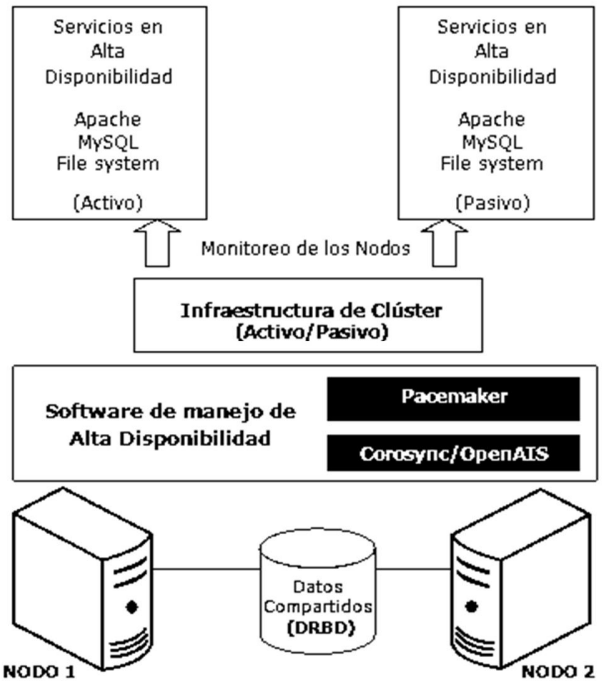

Figura 1. *Esquema del clúster de alta disponibilidad*

3.3 Pruebas de funcionamiento

Para evaluar la efectividad del clúster en producción se realizaron pruebas en maquinas reales y maquinas virtuales, estas últimas se lograron con el uso del software de virtualización *VirtualBox* [19], tanto las máquinas virtuales como las reales, fueron configuradas con características similares en cuanto al sistema operativo, software instalado, configuraciones de las herramientas para la entrega de servicios y esquema de particiones. Una vez establecido y configurado el canal de comunicación en los nodos que integran el clúster, estos se reconocen permanentemente por la red mediante un monitoreo automático constante.

Se estudiaron dos fenómenos que pueden ocurrir en el evento de un fallo, donde una de dichas anormalidades es consecuencia de la otra, siendo estas:

- El tiempo de promoción, para que el nodo secundario pase a primario ante una caída del nodo maestro.
- El tiempo de estabilización, para que el clúster vuelva a la normalidad en términos de disponer de manera correcta los roles activo y pasivo en los nodos.

La tabla 1 muestra cada una de las pruebas realizadas para ese tiempo de promoción y la tabla 2 evidencia cada ensayo para el tiempo de estabilización en los escenarios planteados; cada dato tiene implícito un error como consecuencia de: la velocidad de respuesta del otro nodo a través del canal de comunicación, el instrumento de medición y la velocidad a la hora de finalizar o empezar la toma de las medidas.

Considerando los datos obtenidos en el escenario de las maquinas virtuales, se tiene una media de aproximadamente de 16 segundos para la promoción y la estabilización, considerándose apropiados, ya que es un tiempo relativamente pequeño para el entorno de trabajo; respecto a la desviación también se considera aceptable el dato obtenido de aproximadamente 8 segundos para la promoción y 7 segundos para la estabilización, ya que a pesar de que existan mediciones atípicas, se puede considerar el factor del error en la medida como fundamento para aprobarlos. A nivel de maquinas reales, se nota un cambio mínimo del tiempo de promoción con una media de aproximadamente 13 segundos y un tiempo de estabilización de aproximadamente 15 segundos; esto se puede atribuirle al hecho de que el canal de comunicación entre ambos equipos es dedicado, aunque la desviación de aproximadamente 6 segundos para la promoción y 5 segundos para la estabilización, también se pueden aprobar, al encontrase los tiempos en un intervalo aceptable; considerando estas medidas se puede inferir que el clúster de alta disponibilidad cumple el requisito fundamental de brindar permanentemente los servicios hacia los usuarios.

Tabla 1. *Tiempo de promoción, paso de un nodo secundario a primario*.

Maquinas Virtuales		Maquinas Reales	
No. Toma	Tiempo de Estabilización (s)	No. Toma	Tiempo de Estabilización (s)
1	11,61	1	8,47
2	11,70	2	10,18
3	15,21	3	14,06
4	11,08	4	9,50
5	40,46	5	12,37
6	9,75	6	15,24
7	15,26	7	11,19
8	13,52	8	10,23
9	15,85	9	16,96
10	14,45	10	15,74
11	15,78	11	20,91
12	19,05	12	21,62
13	14,75	13	18,03
14	15,01	14	25,71
15	17,60	15	19,17
Media	16,07	Media	15,29
Desviación	6,95	Desviación	4,93

s = segundos.

Tabla 2. *Tiempo de estabilización, reincorporación de un nodo al cluster.*

Maquinas Virtuales		Maquinas Reales	
No. Toma	Tiempo de Promoción (s)	No. Toma	Tiempo de Promoción (s)
1	8,63	1	6,42
2	10,55	2	9,67
3	10,9	3	12,47
4	10,4	4	7,91
5	11,54	5	8,59
6	19,57	6	6,51
7	9,33	7	13,83
8	9,36	8	12,41
9	27,33	9	10,35
10	9,48	10	7,34
11	18,77	11	20,67
12	8,93	12	18,93
13	21,86	13	23,55
14	29,33	14	14,48
15	33,63	15	27,26
Media	15,97	Media	13,36
Desviación	8,22	Desviación	6,28

s = segundos.

4 MODELO ADMINISTRATIVO

Finalizada la etapa de configuración para la gestión de los servicios, se debe establecer una estructura fuerte al sistema consolidado a nivel de políticas administrativas y de seguridad [20] [21].

4.1 Seguridad

Es Considerado como un proceso de vigilancia permanente, los aspectos que abarcan este componente del modelo administrativo son:

- Hardware: Con el fin de mitigar riesgos y amenazas ante ingresos no autorizados, es necesario el aseguramiento por contraseña del *BIOS* (Basic Input/Output System) y disponer de un espacio restringido a terceros, con llaves físicas para la apertura de gabinete y el frontal de los equipos, para que las modificaciones en el esquema base de operación sean realizados únicamente por el administrador.
- Sistema Operativo: Ningún equipo que se comunica en una red o que sea visible por internet es completamente seguro, es pertinente instalar actualizaciones en el sistema, para mitigar posibles huecos de seguridad, chequeando las implicaciones que pueden acarrear para que no se afecten las aplicaciones, herramientas y configuraciones previas.
- Software: Los errores más comunes en una herramienta son de *overflow* (desbordamiento) y *exploits* (explotación de una vulnerabilidad), por ello es importante asegurar las aplicaciones a nivel de su configuración sin vulnerar la funcionalidad mediante un monitoreando permanentemente.
- Servidor web Apache: Configurar de manera adecuada cada uno de los módulos que compone la herramienta, define la seguridad funcional de esta; deben establecerse el dominio web, los tiempos de respuesta, tiempos de sesión, puertos a disposición, la ruta del directorio raíz, los permisos de los directorios disponibles en el servidor web y mantener un control de privilegios. El protocolo *HTTPS* es necesario configurarse para el cifrado de los datos, se usó la herramienta libre *OpenSSL*, que opera en la capa de transporte e incluye librerías de encriptación del protocolo *SSL* (Secure Socket Layer) y del protocolo *TLS* (Transport Layer Security) [22]; el certificado digital debe ser comprado a una entidad certificadora, cuando se trata de una empresa.
- Gestor de base de datos MySQL; Es altamente recomendable realizar la administración de las bases de datos mediante una interfaz de línea de comandos, evitando herramientas gráficas; a cada una de las bases de datos creadas se les debe asignar un usuario para asegurar la independencia en la gestión de las mismas.
- Lenguaje PHP: En el archivo de configuración tener en cuenta: tiempos de sesión para las solicitudes, tiempos de vida tras inactividad, tiempo de expiración de una solicitud, período de vida para la cookie de navegación y deshabilitar variables globales.
- Alta disponibilidad: La configuración de modo *Activo/Pasivo*, es uno de los aspectos clave en

cuanto a seguridad, ya que la información se encuentra disponible únicamente en el nodo primario, dejando al nodo secundario como respaldo ante una posible condición de error; además, el enlace de red redundante habilita un canal dedicado y aislado de la interfaz que se comunica por la internet.

- Accesos por red: El acceso remoto para realizar labores de configuración, mantenimiento y monitoreo requiere del aseguramiento de puertos, ya que es a través de estos donde se accede al sistema; contar con un Cortafuegos o Firewall es importante para definir aquellos puertos a los cuales se le limitará el acceso. Configurando las reglas en el Cortafuegos *Iptables*, incluido en el sistema operativo se puede gestionar el tráfico de red.

4.2 Usuarios y grupos

La gestión de usuarios se ha basado en roles; mediante la administración de permisos, cada usuario desempeña un papel dentro del sistema. Los roles identificados para esta gestión son:

- Administrador: Este usuario es independiente del root, posee permisos necesarios sobre los archivos y programas para realizar funciones críticas; debido al nivel de privilegios otorgados, no es conveniente que todos los programas sean ejecutados o asociados a este usuario, por tanto se delegan funciones a otros usuarios.
- Usuario de acceso: Dispone de acceso remoto para escalar hacia cuentas de usuario con mayores privilegios y que no dispone de dicha opción. Su rango de operación se limita a su propio directorio.
- Usuario de servicios: Controla las funciones principales del servicio asignado, posibilitando el orden administrativo de cada uno de estos.
- Usuarios jaula: Permiten que los usuarios que requieran un servicio web, ya sea en desarrollo o en producción, tengan acceso a realizar modificaciones en su propio directorio raíz mediante el uso del protocolo *SFTP*.

4.3 Recursos

Además de disponer del clúster de alta disponibilidad, los recursos instalados en los equipos requieren ser gestionados de manera periódica, se deben considerar otros factores que pueden impedir la funcionalidad del sistema, incluyendo los errores humanos. Las acciones que permiten recuperar el sistema considerando este tipo de fallas son:

- Copias de seguridad del sistema: el sistema operativo es el software fundamental i, ya que es allí donde se tienen las configuraciones y las herramientas software para el funcionamiento y correcta prestación de los servicios; mantener un respaldo del SO y de las particiones permite que ante algún error ya sea humano o daño permanente en alguno de los recursos se pueda volver a un estado anterior. Los respaldos se deben realizar en diferentes momentos guardándolos en forma de bitácora en discos internos del sistema y discos externos
- Copias de seguridad de los servicios: Los servicios ofrecidos a los usuarios están sujetos a errores y fallos, que con frecuencia suceden por equivocación humana; es pertinente establecer un esquema de respaldos periódicos como manera de mitigar el problema. De acuerdo al entorno de trabajo, se dispuso un modelo de backups basado en incrementales diarios, respaldos de aquellos archivos con modificaciones posteriores al del día anterior, y un backup completo por semana, copia de todos los archivos que se encuentran dentro del directorio a respaldar, ver Figura 2; estos backups se realizan a horas no laborales para conservar la integridad en la información; como plan de contingencia se mantiene una copia externa, fuera del lugar físico en el que se alojan los equipos. Los backups completos se crean de manera lineal estilo de bitácora; los incrementales sobre-escriben los de la semana anterior.

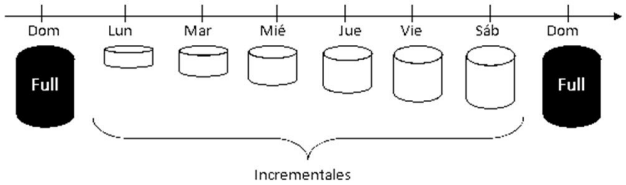

Figura. 2. *Esquema de respaldos periódicos.*

- Revisión de logs del sistema: El sistema operativo guarda registros de los servicios que se ejecutan, es importante que se realice un monitoreo de los eventos que ocurren, para la toma de decisiones y actuar de manera correcta al momento de detectar un comportamiento no esperado. Con el apoyo del software *Logwatch*, cuya licencia es de libre distribución, se realiza un chequeo recopilando de estos eventos del sistema [23].

4.4 Automatización de tareas administrativas

Mediante el uso de scripts Shell y el servicio cron, Linux posibilita la automatización de tareas, desde la generar respaldos hasta notificar la caída de un nodo; esta automatización se puede realizar para que las tareas se ejecuten a ciertas horas y fechas donde además de ganarse eficiencia para la gestión de actividades cotidianas se puede asegurar que la ejecución se realicen correctamente al no estar sujeta a fallos humanos.

4.5 Mantenimiento

Tanto el software como el hardware cambian de manera dinámica, por una parte el software se actualiza mediante parches o nuevas versiones, mientras que el hardware presenta deterioros a nivel de discos duros, ya sea por condiciones del espacio físico o desgaste provocado por el paso del tiempo y uso. Es importante estar preparado para

cualquier fallo y mantener de manera periódica un apoyo técnico a nivel preventivo y correctivo.

4.6 Administración del clúster de alta disponibilidad

El clúster de alta disponibilidad necesita ser monitoreado constantemente para visualizar procedimientos o fallas que se pueden producir a la hora de gestionar o manejar servicios, para ello se dispone de la interfaz de línea de comandos CRM (Cluster Resource Manager), apropiada con instrucciones para mantener un completo control sobre el clúster. Paralelamente usando una tarea automatizada de notificaciones sobre la caída de algún nodo, es posible mantener un control en tiempo real del clúster y asegurar que los servicios se mantendrán disponibles, mediante el trabajo conjunto del administrador y las aplicaciones que proveen la alta disponibilidad.

4.7 Gestión administrativa

Operativamente, los servidores trabajan bajo el modelo cliente-servidor; la información se encuentra centralizada en los servidores y los usuarios acceden a tales contenidos comunicándose por medio de una red [24], para que esta operatividad se efectúe en un contexto organizacional, se han seguido los siguientes principios administrativos [25]:

- Planeación: Realizar planteamientos referentes a expectativas de funciones organizacionales y acciones a futuro.
- Organización: Tomar los objetivos generados en el proceso de planeación y distribuir las actividades según se considere necesario para cumplir el propósito establecido.
- Ejecución: Puesta en marcha de las propuestas establecidas en la planeación y la organización.
- Control: Regular las actividades ejecutadas para que estas se encuentren dentro del marco operacional establecido en la organización.

Aplicando estas directivas, se puede generar un ciclo administrativo en el cual se propicie un entorno de trabajo de optimización continua, en el que las diferentes actividades organizacionales se realicen de manera eficaz y eficiente [26]. La Figura 3, representa el modelo planteado para los procesos internos de la organización.

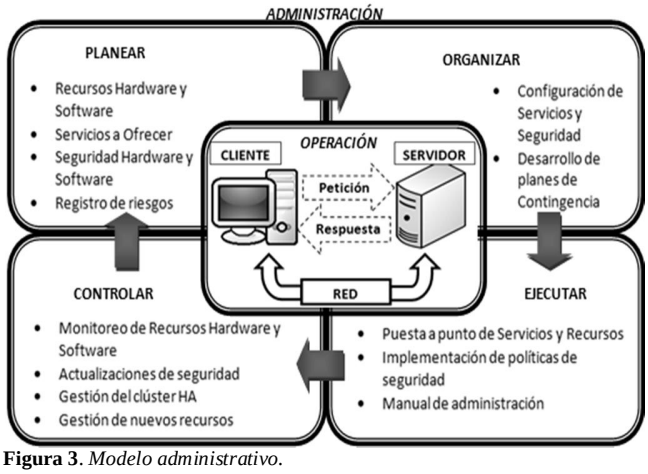

Figura 3. *Modelo administrativo.*

5 NORMATIVIDAD

Establecer un conjunto de normas referentes a la actividad presente en los equipos que indique de manera pertinente los alcances y restricciones de uso y gestión, sirve para que los usuarios a nivel general, tengan conciencia de los límites a los que está sujeta su actividad. Se ha realizado dicha normatividad, con el fin de propiciar un ambiente de trabajo organizado para dar un uso adecuado a los recursos y promover la responsabilidad.

5.1 Normas y políticas

Ser administrador del sistema, implica la realización de actividades que en algunos casos puede comprometer la operación del sistema; los lineamientos que debe seguir este usuario se estipulan en un contrato de confidencialidad en el cual se compromete a regir su trabajo bajo las políticas de seguridad establecidas, comprometiéndose a preservar la información sensible y dar soporte a usuarios que requieran uso de los servidores. El resto de usuarios que tienen acceso a los equipos, deben realizar sus labores de acuerdo a las normativas de uso asociadas a su rol dentro de los servidores mediante la aceptación y firma de un acuerdo de uso de los servicios.

6 REFERENCIAS

6.1 Referencias de Libros

[20] A. Barisani, T. Bader, S. Biles, C. Clark, R. Chiesa, P. Endres, R. Feist, A. Ghirardini, J. Ho, M. Ivaldi, D. Lavigne, S. Presti, C. Low, T. Miller, A. puccetti. *Hacking Exposed Linux: Linux Security Secrects & Solutions*. 3rd ed. ISECOM, McGraw-Hill, 2008

[21] E. Nemeth, G. Snyder, T. R. Hein, B. Whaley. *Unix and Linux Systems Administration Handbook*. 4th ed. Pearson Education, Inc., 2011.

[24] A. S. Tanenbaum. *Redes de Computadoras*. 4th ed. Pearson Education de México, 2003.

[25] I. Chiavenato. *Teoría general de administración*. Elsevier, Río de Janeiro, 2001.

[26] E. M. Fernández. *Introducción a la gestión (Management).* Ed. Universidad Politécnica de Valencia, 1991.

6.2 Referencias en Internet

[1] Sitio web de clusters. Disponible: http://www.clusters.nom.es/ [citado 7 de Enero de 2012]

[2] Sitio web de la comunidad Linalco. Disponible: http://www.linalco.com/hpcc-cluster-de-calculo-alto-rendimiento-linux.html [citado 7 de Enero de 2012]

[3] P. Clavijo. *Clusters de Alta Disponibilidad*. Disponible: http://www.lintips.com/?q=node/119 [citado 7 de Enero de 2012]

[4] Sitio web de la comunidad Linux virtual server. Disponible: http://kb.linuxvirtualserver.org/wiki/Load_balancing [citado 7 de Enero de 2012]

[5] Sitio web de la comunidad Debian. Disponible: http://www.debian.org/ [citado 7 de Enero de 2012]
[6] M. Gelbmann. *Debian is now tthe most popular Linux distribution on web servers*. Disponible: http://www.w3techs.com/blog/entry/debian_is_now_the_most_popular_linux_distribution_on_web_servers [citado 7 de Enero de 2012]
[7] J. Paredes. *Alta disponibilidad para Linux*. Disponible: http://www.ibiblio.org/pub/linux/docs/LuCaS/Presentaciones/200103hispalinux/paredes/pdf/LinuxHA.pdf [citado 8 de Enero de 2012]
[8] Sitio web del proyecto DRBD de la comunidad linbit. Disponible: http://www.drbd.org/ [citado 9 de Enero de 2012]
[9] Sitio web del proyecto Openais. Disponible: http://www.openais.org/ [citado 7 de Enero de 2012]
[10] Sitio web de la comunidad Service Availability. Disponible: http://www.saforum.org/Service-Availability-Forum:-Application-Interface-Specification~217404~16627.htm [citado 9 de Enero de 2012]
[11] Sitio web del proyecto Corosync. Disponible: http://www.corosync.org/ [citado 9 de Enero de 2012]
[12] Sitio web del proyecto Pacemaker. Disponible: http://www.clusterlabs.org/wiki/Pacemaker [citado 9 de Enero de 2012]
[13] Sitio web del proyecto Apache. Disponible: http://www.apache.org/ [citado 20 de Febrero de 2012]
[14] Sitio web del proyecto MySQL. Disponible: http://www.mysql.com/ [citado 20 de Febrero de 2012]
[15] Sitio web del proyecto Tomcat. Disponible: http://tomcat.apache.org/ [citado 20 de Febrero de 2012]
[16] Sitio web del proyecto PHP. Disponible: http://www.php.net/ [citado 20 de Febrero de 2012]
[17] Sitio web del proyecto JAVA. Disponible: http://www.java.com/ [citado 20 de Febrero de 2012]
[18] D. Muhamedagic. *Fencing and Stonith*. Disponible: http://www.clusterlabs.org/doc/crm_fencing.html [citado 9 de Enero de 2012]
[19] Sitio web del proyecto VirtualBox. Disponible: https://www.virtualbox.org/ [citado 20 de Febrero de 2012]
[22] Sitio web del proyecto OpenSSL. Disponible: http://www.openssl.org/ [citado 10 de Enero de 2012]
[23] Sitio web del proyecto Logwatch. Disponible: http://sourceforge.net/projects/logwatch/ [citado 10 de Enero de 2012]

7 CONCULSIONES

El proceso administrativo a nivel de servidores y clúster de alta disponibilidad es una tarea compleja que se puede realizar con el uso de diferentes aplicativos software, lo esencial es la manera como se configuran y se comprometen el sistema; mediante la implementación de políticas y mecanismos de seguridad se provee confiabilidad e integridad para mantener un ambiente administrativo organizado. Estructurar actividades básicas orientadas a un proceso de automatización que liberen la ejecución de tareas repetitivas y permitan al administrador atender otros factores como el mejoramiento de la seguridad y políticas de manejo, monitoreo de la eficiencia del clúster de alta disponibilidad que garantice la prestación efectiva de los servicios. Escalabilidad de servidores y servicios para crecimiento de recursos computacionales académicos.

Este modelo administrativo muestra que se puede brindar un sistema confiable a nivel de prestación de servicios, que ante fallas de algún nodo puede reaccionar de manera automática conservando la integridad de la información del usuario final.

En general, un sistema está sujeto a fallos desde el momento en que se pone a disposición en un entorno de producción, pero con las herramientas y los procedimientos plasmados en este artículo es posible mitigar este tipo de problemas. Con un proceso administrativo organizado y controlado es posible lograr ofrecer un servicio optimo al ambiente que va dirigido, tal como se encuentran en estos momentos los servidores Sistemas y Delfin, en la Escuela de Ingeniería de Sistemas e Informática (EISI) de la Universidad Industrial de Santander (UIS).

8 AGRADECIMIENTOS

Agradecimientos a la Universidad Industrial de Santander y a la Escuela de Ingeniería de Sistemas e Informática por su apoyo permanente.

Agradecimientos a la fundación Raúl Ocazionez y al grupo MEIWEB, que han brindado su apoyado significativo en esta labor investigativa y práctica.

ANEXO 2: ARTÍCULO

ADMINISTRACIÓN DE SERVIDORES: UN ENFOQUE SISTEMICO

SERVER MANAGEMENT: A SYSTEMIC FOCUS

AUTOR 1
Manuel Guillermo Flórez Becerra
M.Sc. Informática
Universidad Industrial de Santander
Profesor Titula
Escuela de Ingeniería de Sistemas
mgflorez@uis.edu.co
COLOMBIA

AUTOR 2
Alexander Barbosa Ayala
Ingeniero de Sistemas
Universidad Industrial de Santander
Administrador de Servidores MeiWeb
Escuela de Ingeniería de Sistemas
alexanderbarbosaayala@gmail.com
COLOMBIA

AUTOR 3
Elkin Darío Muñoz Duarte
Ingeniero de Sistemas
Universidad Industrial de Santander
Administrador de Servidores MeiWeb
Escuela de Ingeniería de Sistemas
elkin.dmd@gmail.com
COLOMBIA

INSTITUCION AUTOR 1
Universidad Industrial de Santander
UIS
Carácter institucional
Carrera 27 Calle 9ª
COLOMBIA

INSTITUCIÓN AUTOR 2
Universidad Industrial de Santander
UIS
Carácter institucional
Carrera 27 Calle 9ª
COLOMBIA

INSTITUCIÓN AUTOR 2
Universidad Industrial de Santander
UIS
Carácter institucional
Carrera 27 Calle 9ª
COLOMBIA

INFORMACIÓN DE LA INVESTIGACIÓN O DEL PROYECTO: Trabajo de grado en la modalidad de trabajo de Investigación titulado "Instalación, administración, configuración e implementación de servidores Linux con énfasis en el desarrollo de un modelo administrativo y la creación de un prototipo de clúster de alta disponibilidad", Fecha de inicio: diciembre de 2010, fecha de finalización: febrero de 2012, Universidad Industrial de Santander, Escuela de Ingeniería de Sistemas, Grupo MeiWeb, Financiado por la Fundación Raúl Ocazionez.

TEMÁTICA ABARCADA POR EL ARTÍCULO: Gestión Tecnológica.

TIPO DE ARTÍCULO: Artículo de Investigación Científica y Tecnológica.

RESUMEN ANALITICO

Creación de un modelo de administración desde una perspectiva sistémica, basado en los fundamentos de la cibernética organizacional, para la administración y uso de servidores de la Escuela de Ingeniería de Sistemas de la Universidad Industrial de Santander (EISI-UIS).

PALABRAS CLAVES

Amplificador
Cibernética organizacional
Filtro
Organización
Sistema Viable

ANALYTICAL SUMMARY.

Creation of an administration model from a systematic perspective, based on organizational cybernetics fundaments, for the administration and use of the servers' Mei Web group from the Systems' engineering School of the Industrial University of Santander (EISI-UIS).

KEYWORDS

Amplifier, filter, organizational cybernetic, organization, viable system

INTRODUCCION

La administración de servidores para uso académico en la EISI-UIS, es una tarea que no se limita únicamente a la gestión de recursos y la adecuación de servicios; ya que estos equipos deben estar disponibles tanto para la oferta, como para desarrollo de nuevos servicios. Es decir, se debe contar con una infraestructura funcional adecuada, para que la labor administrativa pueda efectuarse organizada y controladamente, de tal forma que los desarrolladores y demás usuarios, puedan realizar sus tareas de la forma más adecuada posible. Ante esto, el planteamiento de un modelo de administración desde una óptica organizacional, brinda una serie de medios adecuados para comprender todas las actividades que implican el uso de éstos equipos informáticos.

Una manera de modelar la organización [1], teniendo en cuenta lo anteriormente planteado, es por medio del uso de la metodología del *Modelo de Sistema Viable* [2], propuesta por Stafford Beer, y que utiliza los principios básicos de la cibernética [3], aplicados a las organizaciones; en éste, se trabaja con la idea de interpretar los sistemas sociales como organismos vivos, los cuales tiene sistemas internos que interactúan y realimentan, propiciando que éste se adapte a un ambiente cambiante.

Por tanto, la visión sistémica de la administración de servidores, bajo las propuestas del enfoque cibernético-organizacional [4], pueden brindar los medios adecuados para que se tenga una comunicación apropiada entre los diferentes integrantes de la organización, que de una forma u otra interactúan con dichos servidores, así como mecanismos de regulación de sus actividades, con lo cual, la gestión se realice de manera integral, contando con una planeación oportuna, estando de esta manera preparados para los cambios y necesidades que surgen día tras día.

1. ACERCA DEL MODELO DE SISTEMA VIALBLE

El Modelo de Sistema Viable (MSV) de Beer, surge como una propuesta de la cibernética aplicada a las organizaciones; en éste se observa la organización como un sistema que a su vez contiene una serie subsistemas internos que interactúan entre ellos y tienen mecanismos de regulación, que propician el equilibrio interno de la organización [5].

Las características fundamentales [6] que debe tener una organización que opere bajo el modelo de sistema viable son:

- La organización debe ser comprendida como un sistema, que cuente con niveles o subsistemas que se auto-regulan y con capacidad de decidir el momento y la forma en que realiza su acción.
- La administración no es centralizada, por lo tanto, cada nivel es considerado autónomo y debe generar respuesta o salidas hacia otros subsistemas de la organización, para que de esta manera se haga posible su gestión.
- En el modelo, la organización se debe considerar como un todo funcional, mayor a la suma de sus partes, con lo que los subsistemas deben contar con entradas, salidas y medios de realimentación de la información.
- La organización no es independiente del entorno en el que se encuentra y debe contar con medios que le permitan adaptarse a los cambios de éste.
- Se debe tener claro el límite organizacional del sistema, es decir, debe tener claramente definidas las actividades fundamentales (el propósito de la organización) para su adecuada administración.
- Aplicación de mecanismos para control de variedad (cantidad de información que pasa de un subsistema a otro).

Además de las anteriores características, se debe tener en cuenta que los sistemas viables deben contar con los siguientes tres elementos básicos [7]:

- Las operaciones o procesos.
- La Administración.
- El ambiente o entorno de la organización.

Todo esto se articula en la funcionalidad cotidiana de la organización, teniendo en cuenta los diferentes canales de comunicación y demás mecanismos propuestos, que siendo aplicados, pueden dar a la gestión organizacional un nivel de competitividad acorde a los diferentes retos y exigencias que se le puedan presentar. A continuación se muestra en más detalles de la composición general del MSV.

2. COMPONENTES DE MODELO DE SISTEMA VIABLE

Los Sistemas viables se encuentran compuestos por cinco subsistemas [8] que a su vez son viables, los cuales interactúan entre ellos por medio de canales de comunicación regulados, visibles en la Fig. 1, que hacen posible mantener la organización articulada pero con suficiente autonomía en sus diferentes sistemas internos.

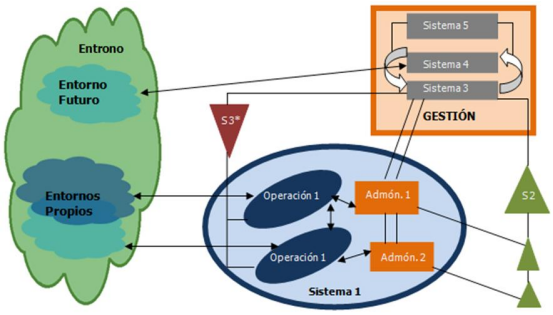

Fig. 1. Adaptación modelo general de sistema viable

Sistema Uno: Es el subsistema en el cual se realizan las operaciones primarias de la organización, como lo son la producción de bienes o servicios. Cada sistema uno se encuentra en un entorno específico o entorno propio.

Sistema Dos: Representa los canales de manejo de la información acerca de las operaciones realizadas en el sistema uno. Este opera en el dominio administrativo y provee de información importante acerca de la operaciones del sistema uno al sistema tres, con lo

cual la administración logra regular las actividades realizadas en el sistema uno.

Sistema Tres: Es el encargado de generar las diferentes estructuras de control que propician un ambiente interno estable, tales como reglas, derechos y responsabilidades del sistema uno que son monitoreadas desde el sistema tres*. Además, el sistema tres provee un canal entre las operaciones de los sistemas cuatro y cinco.

Sistema Tres:* Representa el canal de monitoreo de las operaciones del sistema uno desde el sistema tres, tal información puede ser utilizada por los sistemas cuatro y cinco para la toma de decisiones.

Sistema Cuatro: Es el encargado de generar escenarios en los cuales se pueda evaluar la organización a futuro; esto se representa relacionado con un entorno futuro, pues en este sistema se crea un contexto en el cual se pueda responder a los cambios en el entorno adecuadamente y a los retos y oportunidades que estos representan.

Sistema Cinco: Es el encargado de establecer las políticas y la toma de decisiones final. Debe facilitar un ambiente de interacción en el cual los sistemas tres y cuatro puedan llegar a acuerdos que favorezcan el normal desarrollo de las actividades de la organización.

En este modelo todas las actividades organizacionales se realizan dentro de un entorno en el que la organización misma no se debe considerar aislada de este; de allí que este modelo, presenta una forma de pensar la administración dinámicamente y con capacidad de adaptación a los cambios.

Todas las líneas de comunicación entre los sistemas internos, están sujetas a la *ley de variedad requerida* para el establecimiento de un sistema de control, la cual cuenta con filtros para que el flujo de información del sistema más general, sea tomado por el más particular y amplificadores para la comunicación del más particular al más general. De esta forma, se puede lograr una comunicación más efectiva y un equilibrio natural entre los diferentes sistemas de la organización; por ejemplo, los datos que fluyen desde las operaciones a la administración son filtrados para que este último pueda tomar los datos fundamentales para la toma de decisiones sobre las operaciones, así mismo, la información que fluye desde la administración a las operaciones cuenta con amplificadores, que apoyan la comunicación de tales decisiones al nivel operativo.

3. UN CASO CONCRETO: DIEÑO DE UN MSV PARA LA ADMINSITRACIÓN DE SERVIDORES EN LA EISI-UIS.

3.1 Reconocimiento de la organización a modelar

En la Escuela de Ingeniería de Sistemas de la Universidad Industrial de Santander, se adquirieron dos equipos servidores destinados exclusivamente a la oferta y desarrollo de servicios web. Estos fueron configurados y puestos en funcionamiento de acuerdo a dichos requerimientos. No obstante, para logra que se formara un ambiente de trabajo interno adecuado, administrativamente se plantearon estrategias en cuanto a normas, esquemas de monitoreo y demás formas de control, con las cuales la gestión de uso de los equipos se diera de forma correcta y controlada, pero brindando suficiente autonomía a los miembros de los grupos de trabajo para la realización sus actividades.

Uno de los planteamientos principales fue la creación de un modelo de administración, el cual se encuentre articulado con los mecanismos y políticas de control y demás normatividad de uso de los servidores, en relación con los diferentes actores internos de la organización.

Por tanto, realizar un modelo desde la perspectiva de sistema viable, puede brindar el apoyo administrativo necesario para el entorno de operación planteado, englobando el propósito fundamental de la organización y su proyección a futuro, dado a que si se tiene un orden claro de los roles de todos aquellos que utilizan los equipos y el establecimiento de canales óptimos de comunicación, se hace posible que tales recursos informáticos se utilicen de una forma correcta y responsable.

3.2 Diseño del modelo de sistema viable organizacional.

Para el planteamiento del modelo, se ha tenido en cuenta la información recopilada acerca de la organización a modelar, revisado sus diferentes subsistemas presentes para relacionarlos según las características estructurales acerca del modelo de sistema viable. Igualmente, se ha delimitado el ambiente en que desarrolla sus actividades la organización, sus diferentes aspectos funcionales, los canales de comunicación el entorno y los entornos propios.

En seguida, se muestra en mayor detalle la descripción de cada elemento del sistema viable de la organización estudiada, condensando gráficamente dicha información en la Fig. 2.

Entorno Relevante: Es la Escuela de Ingeniería de Sistemas. Los desarrolladores y los servicios hacen parte de esta escuela. En el modelo de sistema viable, se destaca que las fronteras del entorno relevante son borrosas, por tanto, el entrono es graficado de manera irregular, ya que este es cambiante. Para este caso, se puede decir que los servicios desarrollados pueden ser ofrecidos a un entorno más allá de las fronteras delimitadas, es decir, más allá de la EISI-UIS, pero sujetos a sus normas misionales.

Sistema Uno: En este caso, las tareas primarias son el desarrollo y ofrecimiento de servicios orientados a la web. Como todas las operaciones, de lo que se considera sistema uno, son desarrolladas dentro de un ambiente propio, para este caso, tal entorno son los dos equipos servidores de trabajo, ya que son estas máquinas en las cuales se prueban los proyectos en desarrollo y se alojan los servicios ofrecidos. Es de resaltar que todos los servicios alojados no son de uso comercial, pues se encuentran en un ambiente académico.

Podría pensarse que el entorno, puede ser el sitio geográfico de trabajo dentro de la EISI-UIS, por ejemplo, una oficina, pero en

este caso se está hablando de desarrollo de servicios a nivel de software, que no son físicamente tangibles; por tanto, se debe trabajar la ideal global de alojamiento de servicios en los equipos, para disponer de estos en la web.

Teniendo lo anterior clarificado, es de resaltar que todas las operaciones realizadas deben tener un medio de regulación, es decir, debe existir una coordinación de proyecto, desde la cual se hagan los procesos de planeación y toma de decisiones para la orientación adecuada del proceso de desarrollo o administración del servicio web y éste no se desvíe del propósito principal.

La actividad de administración de los procesos, es llevada a cabo tanto por los directores de proyecto como de los estudiantes que desarrollan el proyecto, pues es una actividad conjunta en la que ellos interactúan intercambiando ideas y tomado las decisiones que consideren adecuadas para que el servicio web cumpla con los objetivos planteados.

Sistema Dos: Es el canal de de comunicación entre los administradores de los recursos informáticos y los de los servicios. Este es un subsistema muy crítico, porque es en este punto donde se establecen las pautas para la realización de tareas dentro de los servidores, luego, según sea la normatividad establecida, se llegan a acuerdos de uso en los cuales, los administradores de los equipos, puede establecer pautas en el ofrecimiento de soporte para la realización de ciertas tareas para que los servicios, según sea el caso; estas actividades de apoyo administrativo puede son la creación de respaldos de los datos de los servicios, accesos a las bases de datos, principalmente.

Sistema Tres: Este subsistema se encuentra representado por la administración de los recursos informáticos, ya que sirve como puente de interacción entre los demás miembros del grupo de gestión principal (Grupo de planeación y Director del Grupo) y los que gestionan las operaciones. Su canal de comunicación es el sistema dos, con lo cual se mantiene regulado el sistema organizacional y se pueden desempeñar todas las operaciones con autonomía pero acogiéndose a los acuerdos normativos establecidos.

Los administradores de los servidores, son los que poseen el control principal de los equipos, por tanto generan la normatividad de uso y los planes de contingencia para los equipos a partir de la orientación y el consenso de ideas con los otros miembros del grupo principal de gestión.

Sistema Tres*: Es un sistema de apoyo para los administradores de recursos informáticos (sistema tres), donde se establecen las actividades de monitoreo, en el cual se busca garantizar que las operaciones hechas se encuentren dentro de los parámetros de uso establecidos.

En este sistema está el monitoreo a través de los registros de sistema de los servidores y aplicación de los planes de contingencia, por si se presentan problemas o fallos en los equipos por diferentes razones, que pueden ser independientes a las actividades operacionales, y así pueda actuarse de manera oportuna y afectar lo menos posible la prestación y desarrollo de los servicios.

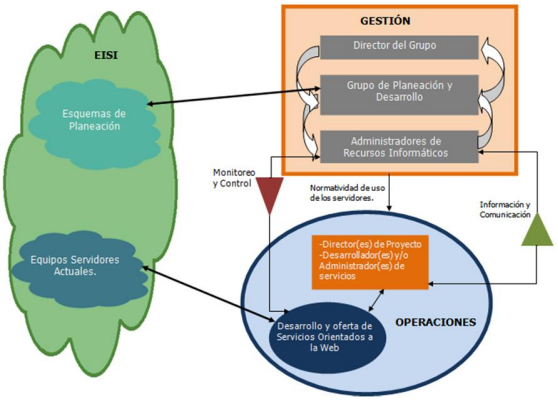

Fig. 2. Modelo de sistema viable planteado para el caso estudiado.

Sistema Cuatro: Es un grupo de planeación. En este se encuentran los directores de proyectos, que puede ser el director del grupo (al ser un miembro activo de la EISI-UIS), y los estudiantes que están dispuestos a desarrollar tales proyectos planeados. Así mismo, la planeación no se limita sólo a crear escenarios en los cuales se puedan desarrollar nuevos servicios, sino en la medida que se disponga de nuevos equipos informáticos, tanto el director del grupo como los administradores pueden planear su uso a futuro de la mejor manera posible, planteando en cada caso escenarios de riesgos y oportunidades que se puedan presentar e ir generando planes de contingencia según sea el caso evaluado.
Por tanto, en este grupo de planeación, interactúan tanto directores, administradores y desarrolladores para adaptarse a las condiciones y retos que se presenten con el paso del tiempo. En este sistema al ser de visión hacia futuro, se representa conectado a un entorno futuro, lo cual indica que la actividad de planeación se encuentra sujeta a cambios en el entorno actual.

Sistema Cinco: En este se encuentra el director del grupo, su actividad principal gira en torno a la toma de decisiones finales, de acuerdo a la información que se le suministra desde los demás subsistemas. Además, el director al ser un miembro activo de la EISI, también puede ser director de proyectos y tener contacto directo en el sistema de operación (sistema uno), por tanto, puede actuar en diferentes campos administrativos según le sea requerido.

3.3 Mecanismos de control aplicados.

Para que el modelo planteado anteriormente se considere un sistema viable, los canales de comunicación deben encontrarse auto-regulados, para de esta forma, contar con una comunicación efectiva, de acuerdo a la ley de variedad requerida antes mencionada. El diseño de los filtros y los amplificadores [9] en las líneas de comunicación se realizó de acuerdo a criterios administrativos de manejo de información de manera equilibrada, por ejemplo, como no toda la información del entorno debe ser trasmitida al grupo de operaciones, estos deben contar con criterios de selección de la información para captar sólo la que

necesita, de igual manera, la administración maneja todos los procesos de la parte operativa, así que debe contar con los medios para que sus propuestas lleguen amplificadas al contexto de desarrollo, logrando así una adecuada administración. Estos criterios se encuentran representados en la Fig. 3.

En esta figura se evidencia que la comunicación entre las partes se encuentra basada en procesos de filtrado y amplificación según sea el rol desempeñado dentro de la organización; de igual forma, en la tabla inferior de la misma figura, se presenta el regulador implementado para cada línea de comunicación. Con la creación de estos mecanismos de comunicación, se busca generar estabilidad general en el ambiente de trabajo, lo cual determina la efectividad en todos los procesos organizacionales.

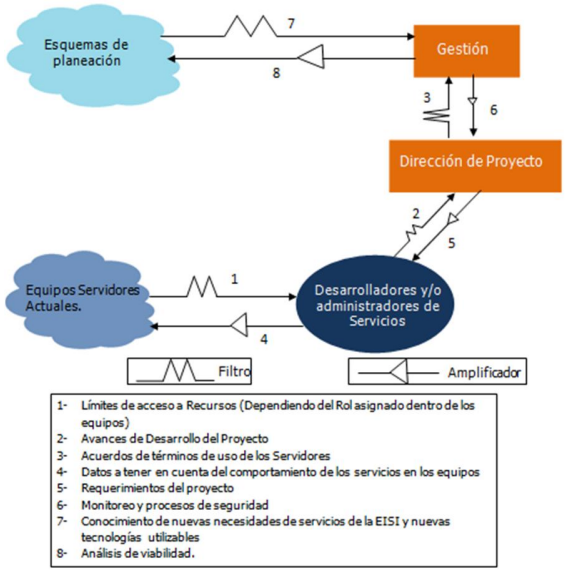

Fig. 3. Sistema de control de la comunicación

4. CONCLUSIONES

El apoyo en las teorías sistémicas, en especial de la cibernética organizacional, para la generación de un modelo de administración, brinda una perspectiva general muy importante para la gestión de los diferentes procesos internos, a su vez, tiene en cuenta la interacción con el entorno y la planeación requerida para afrontar de la manera más adecuada posible los cambios que se presentan en el entorno en el cual desempeña sus funciones la organización.

Es de resaltar, que el modelo planteado para el caso de la gestión de los servidores de la EISI-UIS, puede estar sujeto a optimizaciones, en cuanto al nivel de detalle de cada subsistema y sus canales de comunicación, pues como en todo sistema social, su representación gráfica esté ligada a diferentes puntos de vista y paradigmas socio-culturales de los diseñadores del modelo y demás miembros de los grupo de gestión.

5. REFERENCIAS BIBLIOGRAFICAS

[1] Morgan, Gareth. Images of Organization. Sage Publications LTD. London UK, 1986.

[2] Beer Stafford. Brain of the Firm. 2nd ed, Chichester Wiley, London, 1981

[3] Wiener, Norbert. Cybernetics: or Control and Communication in the animal and the Machine. Wiley, New York. 1961.

[4] Beer, Satafford. The hearth of the Enterprise. John Wiley & Sons, London 1979.

[5] Andrade, Hugo. Dyner, Isaac. Espinosa, Ángela. López, Hernán. Sotaquirá, Ricardo. Pensamiento sistémico: Diversidad en búsqueda de Unidad. Universidad Industrial de Santander, 2001

[6] Espejo, Raúl. Harnden, Roger. The Viable System Model: Interpretations and Applications of Stafford Beer's VSM.. John Wiley & Sons, Chichester, London, 1989.

[7] Rivera, Enrique. Ossa, Catalina. Opazo, Daniel. Vidal, Sebastián. Cybersyn: sinergia cibernética. Santiago de Chile, 2006. [Online]. Disponible: http://www.cybersyn.cl/imagenes/documentos/textos/cybersyn_sinergia_cibernetica.pdf.

[8] Espejo, Raúl. Conceptos y Prácticas de control; Una experiencia concreta: La dirección industrial en Chile. Corfo, Santiago de Chile, 1973.

[9] Ashby, William Ross. An Introduction to Cybernetics. London, 1956.